2019

SWEF DISTANCE SUPPORT HUB

Diaz, Uriel; Gordillo, Juan C.; Gorospe, Jonathan-Marc A.; Ketterling, Wade E.; Marquezdealba, J; Marte, Victor; Voas, Kevin S.

Monterey, CA; Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

SYSTEMS ENGINEERING CAPSTONE REPORT

SWEF DISTANCE SUPPORT HUB

by

Uriel Diaz, Juan C. Gordillo, Jonathan-Marc A. Gorospe,
Wade E. Ketterling, J Marquezdealba, Victor Marte,
and Kevin S. Voas

December 2019

Advisor: Mark M. Rhoades
Co-Advisor: Bryan M. O'Halloran

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2019	**3. REPORT TYPE AND DATES COVERED** Systems Engineering Capstone Report

4. TITLE AND SUBTITLE SWEF DISTANCE SUPPORT HUB	**5. FUNDING NUMBERS**
6. AUTHOR(S) Uriel Diaz, Juan C. Gordillo, Jonathan-Marc A. Gorospe, Wade E. Ketterling, J Marquezdealba, Victor Marte, and Kevin S. Voas	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

The Naval Surface Warfare Center Port Hueneme Division (NSWC PHD) requires a redesign of the Surface Warfare Engineering Facility (SWEF) to act as a central hub for real-time Navy fleet combat systems distance support from the applicable In-Service Engineering Agent (ISEA). This study produced two architectures for the SWEF-Hub. The first architecture is implementable within a short time and largely creates the central communications station and details activities that it will perform. The second architecture, implementable in the long-term, employs advanced technological concepts including machine learning and condition-based maintenance to help the warfighter perform effective and timely equipment preventative and corrective maintenance, provide the health status of every ship to the departments within NSWC PHD, and streamline decision-making processes and provide enhanced distance support. In addition, SWEF-Hub will provide the capabilities to allow secure data analysis, system software updates, and predictive system analysis. The goal of the SWEF-Hub redesign is to provide secure, efficient use of distance support resources that will result in increased productivity of maintenance and support personnel, increased system availability, increased situational awareness concerning the status of critical systems, and improved customer service to the warfighter.

14. SUBJECT TERMS Surface Warfare Engineering Facility, SWEF, hub, distance support, DS, data analysis, machine learning, ship health, Navy combat systems, collaborate	**15. NUMBER OF PAGES** 269
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

SWEF DISTANCE SUPPORT HUB

Uriel Diaz, Juan C. Gordillo, Jonathan-Marc A. Gorospe,
Wade E. Ketterling, J Marquezdealba, Victor Marte, and Kevin S. Voas

Submitted in partial fulfillment of the
requirements for the degrees of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING

and

MASTER OF SCIENCE IN ENGINEERING SYSTEMS

from the

NAVAL POSTGRADUATE SCHOOL
December 2019

Lead Editor: Wade E. Ketterling

Reviewed by:
Mark M. Rhoades
Advisor

Bryan M. O'Halloran
Co-Advisor

Accepted by:
Ronald E. Giachetti
Chair, Department of Systems Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The Naval Surface Warfare Center Port Hueneme Division (NSWC PHD) requires a redesign of the Surface Warfare Engineering Facility (SWEF) to act as a central hub for real-time Navy fleet combat systems distance support from the applicable In-Service Engineering Agent (ISEA). This study produced two architectures for the SWEF-Hub. The first architecture is implementable within a short time and largely creates the central communications station and details activities that it will perform. The second architecture, implementable in the long-term, employs advanced technological concepts including machine learning and condition-based maintenance to help the warfighter perform effective and timely equipment preventative and corrective maintenance, provide the health status of every ship to the departments within NSWC PHD, and streamline decision-making processes and provide enhanced distance support. In addition, SWEF-Hub will provide the capabilities to allow secure data analysis, system software updates, and predictive system analysis. The goal of the SWEF-Hub redesign is to provide secure, efficient use of distance support resources that will result in increased productivity of maintenance and support personnel, increased system availability, increased situational awareness concerning the status of critical systems, and improved customer service to the warfighter.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

24/7	Twenty-four hours a day / seven days-a-week
A	Analysis
AA	Aegis Ashore
AegisTT	Aegis Technical Team
API	Application Program Interfaces
BMD	Ballistic Missile Defense
BUMED	Bureau of Medicine (NAVMED)
BUPERS	Bureau of Personnel
CASREP	Casualty Report
CBM	Condition-Based Maintenance
CBM+	Condition-Based Maintenance Plus
CG	Guided Missile Cruiser
CNSF	Commander, Naval Surface Force
COA	Course of Action
ConOps	Concept of Operations
D	Demonstration
DDG	Guided Missile Destroyer
DE	Directed Energy
DESIL	Directed Energy System Integrated Laboratory
DOD	Department of Defense
DoDI	Department of Defense Instruction
DON	Department of the Navy
DS	Distance Support
DStR	Stakeholder Requirement, Shall Do
DSyR	System Requirement, Shall Do
EN	Effective Need
EW	Electronic Warfare
FFBD	Functional Flow Block Diagram

FISMA	Federal Information Security Management Act
FR	Functional Requirement
GDSC	Global Distance Support Center
HBSS	Host Based Security System
HM&E	Hull, Mechanical and Electrical
HMI	Human Machine Interface
HStR	Stakeholder Requirement, Shall Have
HVAC	Heating, Ventilation & Air Conditioning
I	Inspection
IA	Information Assurance
IAVA	Information Assurance Vulnerability Alert
ID	Identification
INCOSE	International Council on Systems Engineering
IPR	In-Progress Review
ISEA	In-Service Engineering Agent
IT	Information Technology
IWS	Integrated Warfare System
LCS	Littoral Combat Ship
LCSRON	Littoral Combat Ship Squadron
LDSC	Littoral & Strike Warfare Distance Support Center
LPD	Amphibious (L) Platform Dock
MDA	Missile Defense Agency
ML	Machine Learning
MOE	Measure of Effectiveness
MOP	Measure of Performance
MOS	Measure of Suitability
MPCMS	Machinery Propulsion Control and Monitoring System
MPSF	Mission Package Support Facility
MRC	Maintenance Requirement Card
NAVMED	Naval Medicine Command

NAVSEA	Naval Sea Systems Command
NB	Naval Base
NBVC	Naval Base Ventura County
NFR	Non-Functional Requirement
NIC	Naval Installations Command
NIWC	Naval Information Warfare Center
NOC	Notice of Completion
NSWC	Naval Surface Warfare Center
NSWCPHDINST	Naval Surface Warfare Center Port Hueneme Instruction
OPNAV	Operational Navy Command
OPORD	Operational Order
OpsCon	Operational Concept
OS	Operating System
PEO	Program Executive Office
PHD	Port Hueneme Division
PMS	Planned Maintenance System
PN	Primitive Need
POC	Point of Contact
RAM	Random Access Memory
RMC	Regional Maintenance Center
RMF	Risk Management Framework
RVTM	Requirements Verification Traceability Matrix
S2E	Sailor to Engineer
SDREN	Secure Defense Research and Engineering Network
SE	System Engineering
SIEM	Security Information and Event Management
SIPR	Secure Internet Protocol Routing
SME	Subject Matter Expert
SOI	System of Interest
SPAWAR	Space and Naval Warfare

St	Stakeholder
StR	Stakeholder Requirement
SWEF	Surface Warfare Engineering Facility
SyR	System Requirement
T	Test
T&E	Test and Evaluation
TASKORD	Task Order
TPM	Technical Performance Measure
USN	United States Navy
U.S.	United States
VAB	Variable Action Buttons

EXECUTIVE SUMMARY

As part of an effort to improve the combat systems support provided to the Navy, Port Hueneme Division leadership is investing in innovative concepts that will make it possible. One of those concepts is the creation of a support center where all combat system distance support requests would be managed.

In recent years, the U.S. Navy has set forth an effort to reduce manning across the fleet. This has created deficiencies in the operation and maintenance of combat systems equipment by the end user. These deficiencies have overloaded the combat systems In-Service Engineering Agent (ISEA) personnel by lending support to the warfighter in ways that are not economically feasible or sustainable.

This capstone project addresses the need of the Naval Surface Warfare Center Port Hueneme Division (NSWC PHD) to redesign the Surface Warfare Engineering Facility (SWEF). The goal of redesigning SWEF is to provide the fleet with fast and sophisticated distance support by supplying the necessary technology to maintain combat systems readiness on every U.S. Navy ship regardless of their geographical location. The intention is for the redesigned SWEF to accomplish improved distance support by interfacing with the warfighter through a centralized combat system support center where personnel utilizing sophisticated computer systems and databases can assist the navy. This common interface is entitled SWEF-Hub. The SWEF-Hub provides combat systems distance support in real time by securely transferring information between the facility and the ships in order to assist sailors in the execution of corrective and preventive maintenance, and to provide the means to upload automated software upgrades efficiently. The intended results include shorter combat system equipment downtimes and improved ship readiness.

The SWEF-Hub team generally followed the INCOSE handbook system engineering (SE) processes in the development of the SWEF-Hub architectures.

The first item the SWEF-Hub team developed was a problem statement to capture and explain the requirements of NSWC PHD. The problem statement is:

> The Naval Surface Warfare Center Port Hueneme Division (NSWC PHD) requires a redesign of the Surface Warfare Engineering Facility (SWEF) to act as a central hub for future real-time Navy combat systems distance support. This SWEF-Hub will employ advanced technological concepts to assist the warfighter to perform effective and timely preventative and corrective maintenance to their equipment. The hub will furnish NSWC PHD with the tools necessary to reduce the need to field on-site field engineers while providing the health status of combat systems on every ship to the departments within NSWC PHD. The SWEF-Hub will incorporate a means to collaborate in real time with the U.S. Navy's leadership and fleet sailors to streamline decision-making processes. The goal of the SWEF-Hub redesign is to provide a more efficient use of support resources that will result in increased productivity of the maintenance and support personnel, increased situational awareness concerning the status of combat systems, and improved customer service to the warfighter.

The second item developed was a technical approach to address the problem. The Systems Engineering plan used to develop the SWEF-Hub on this capstone was the Vee Model. Due to time constraints and project scope, the SWEF-Hub team only executed the technical design process, a portion of the left-hand side of the Vee Model as shown in Figure ES-1.

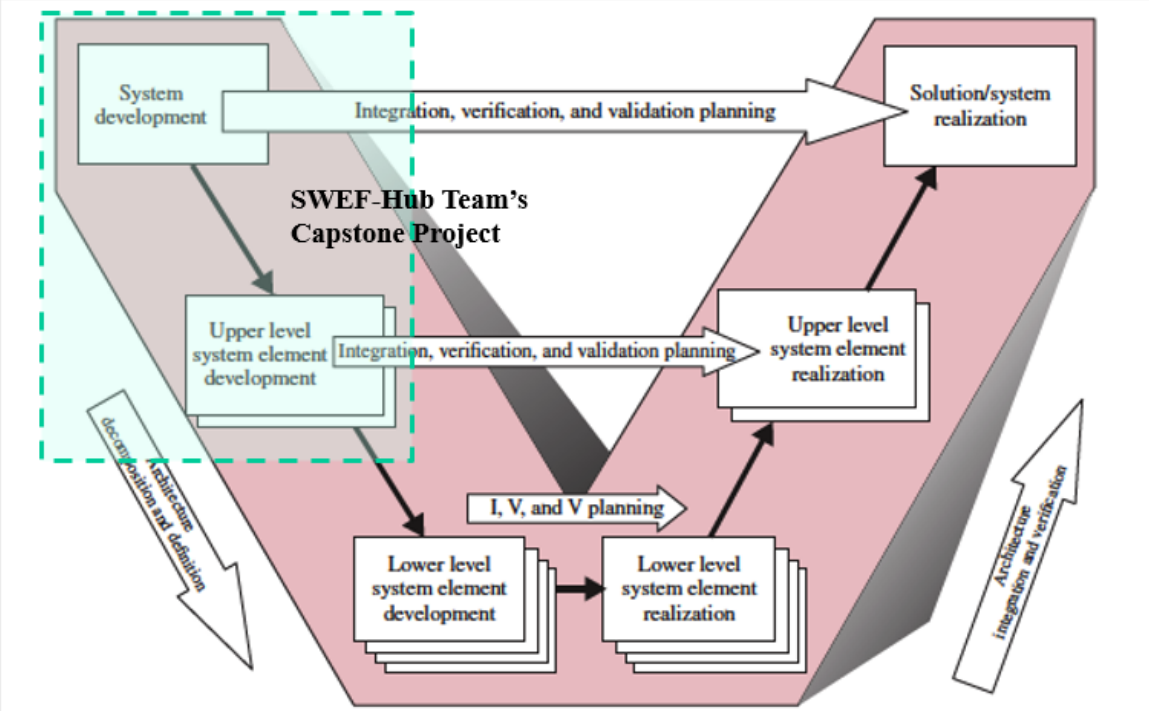


FIGURE 3.6 Vee model. Derived from Forsberg et al. (2005), Figure 7.10. Reprinted with permission from Kevin Forsberg. All other rights reserved.

Figure ES-1. Vee Model. Adapted from INCOSE (2005).

The third item developed by the team was the mission analysis for the SWEF-Hub that included:

- The problem statement refinement; the context diagram.
- The concept of operation definition.
- The SWEF-Hub operations.
- External organizations that make up the support for the fleet combat systems. These include NSWC Crane, NSWC Corona, Naval Information Warfare Command (NIWC), NSWC Dahlgren, Missile Defense Agency (MDA), Naval Base Ventura County (NBVC) Point Mugu, NBVC San Nicolas Island, and NSWC PHD.
- The SWEF-Hub data fusion and analysis capability.

- The major stakeholders.

The fourth item the team developed was the stakeholder needs requirements. During this process, the operational concept (OpsCon) was developed as well as other life cycle processes. After the stakeholders' requirements and the OpsCon were developed, the following actions were conducted: identify functional requirements, create functional hierarchy, establish Measures of Effectiveness (MOE's), and produce the system requirements definition.

The fifth item developed was the system requirements for the SWEF-Hub. The system requirements definition system engineering (SE) process took the refined stakeholder requirements and transformed them into system requirements. This process was accomplished by identifying the system functions, creating and analyzing the systems requirements, and then identifying the system functional interfaces. The process culminated in the management of systems requirements.

The sixth and final item in the SE process developed by the SWEF-Hub team was the system architecture for the SWEF-Hub. Two separate architectures were developed, a near-term architecture that could be implemented within a three-year timeframe, and a long-term architecture with a ten-year implementation timeframe. The SWEF-Hub architectures were developed using Excel and Innoslate. These architectures finalize the technical design process that can be used to continue onto the right side of the Vee Model. Six steps were executed in the development of the SWEF-Hub architectures:

1. Prepare what is necessary to define the architecture
2. Create the viewpoints of the architecture
3. Create models and views of the architecture
4. Show the relationship between the architecture and the design
5. Evaluate the different architectural candidates
6. Manage the architecture process and the architecture.

The SE process proved to be effective in providing an architecture that satisfies the stakeholders' needs.

The near-term SWEF-Hub architecture is feasible with current technologies. However, implementation will require shipboard process changes that flow in parallel with the SWEF-Hub processes. The long-term SWEF-Hub architecture was developed under the directive to utilize likely improvements in technological capabilities in the relatively near future, with the goal of implementing the system in the ten-year timeframe. Significant lack of technology improvement would create risk for the implementation of the long-term architecture. Additionally, shipboard changes in equipment and processes would be required to successfully implement the long-term SWEF-Hub architecture; risk is increased if these changes are not developed in parallel with the SWEF-Hub.

Reference

International Council on Systems Engineering (INCOSE). 2015. *Systems Engineering Handbook*, 4th ed. San Diego, CA: INCOSE.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

The SWEF-Hub team would like to extend their sincere thanks to the many people who contributed, directly or indirectly, to the success of this capstone project.

The team expresses their regards for the support and patience of their families, which was the most important influence toward the successful completion of this two-year-long program and capstone project.

The team would like to thank their advisors, Mr. Mark Rhoades and Dr. Brian O'Halloran, for their guidance. The team would also like to thank John (Mike) Green, from NPS, for his leadership, inspiration, and instruction throughout several of our classes. Special thanks to Colette O'Connor from the NPS Graduate Writing Center for reading and proofing many revisions to this report.

The SWEF-Hub team would finally like to recognize Mr. Mike Horton, Mr. Jeff Koe, Mr. Timothy Jones, and Mr. Al Gabertan of the Naval Surface Warfare Center, Port Hueneme Division (NSWC PHD).

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The United States Navy (USN) places fleet elements worldwide for a multitude of purposes. The majority are combat elements with multiple combat systems contained on each platform. Centralized combat system support groups composed of In-Service Engineering Agents (ISEAs), logistics, and maintenance and repair facilities support the individual combat systems. The support groups utilize a combination of distance support and in-person technical support visits to help the warfighters maintain their combat systems readiness. Each support group collects system health/metrics data as it sees fit.

Currently the combat system support groups are decentralized. Each support group uses its own communications interfaces and methods of delivering support, resulting in inconsistent levels of support. Infrastructure development repeats across numerous separate physical installations, resulting in higher support costs. Warfighter support is not optimized or consistent across all combat systems; support systems for some combat systems are well organized and carried out efficiently, while others tend to receive support resources only when problems appear. As such, this has been identified as an interoperability issue within the fleet. For combat system support, good interoperability would include standardized methods of communications, consistency of support levels across the different combat systems, and clear pathways between the fleet elements and the sources of support.

Each combat system support group works individually to develop approved cyber security for its systems and communications methods. Multiple interface systems with multiple cyber security methodologies exist across the different support groups. Multiple systems using multiple methods tend to increase system operational expenses.

This capstone report provides a system architecture for a centralized Surface Warfare Engineering Facility hub (SWEF-Hub). The SWEF-Hub is an interoperability solution that enables combat system support groups to interface with the warfighters' maintenance and support personnel through a common interface. The SWEF-Hub allows for real-time Navy combat systems distance support through a robust and secure

communications link between ships and the combat systems support groups through a centralized support center. The SWEF-Hub provides multiple benefits, including both improved situational awareness of fleet-wide combat system readiness and improved combat systems availability.

A. BACKGROUND

The USN benefits from effective support of all combat systems. Combat systems support groups must support the combat elements; they provide assistance to the warfighters when needed in order to maintain combat system availability at a superior level. While not an all-inclusive list, effective support includes efficient use of resources, consistency of support methods, and the ability to efficiently accomplish maintenance and support actions; efficient support includes rapid feedback between support elements and the warfighters to maintain the combat systems. Efficiency improves when there is a program in place to analyze data collected during maintenance actions and there are methods in place to instigate improved maintenance processes for the warfighters.

USN policy has been emphasizing smaller crew sizes and the accomplishment of most significant maintenance actions to occur at shore-based maintenance facilities. These separate policies have tended to decrease the onboard system maintenance knowledge base and inherent (without support) shipboard repair capability. Due to these policies, the importance of distance support in afloat combat system maintenance and repair operations has increased.

Information network communications throughout the Navy have improved and increased. Data bandwidth limitations decrease and the speed of information transmission increases as fleet communications technology improves over time. Increases in onboard computational power provide significant capabilities for data analysis, simulation, and training. Real-time communications between fleet sailors and combat systems support groups is gradually becoming a realistic option. Innovations in virtual reality visualizations and real-time communications allow the potential for one-on-one warfighter support during maintenance and repair actions. This sort of support interface potentially enables a reduction in on-site technical assistance requirements.

The drive for information assurance (IA) through cyber security methods affects all data communications fleet-wide. Development of IA for communications networks for multiple combat systems support groups is resource intensive and leads to inconsistencies in implementation of the cyber security methods, as well as excessive redundancies in infrastructure. Centralization of communications nodes through a single hub helps to both simplify development and IA support of secure interfaces and reduce resource use.

In combination with IA and increases in data transmission capability, the possibility of remotely providing afloat combat systems with operational software enhancements or revisions exists. Improved real-time distance support potentially allows the combat systems support group personnel to work directly with the warfighters' support and maintenance personnel to ensure the proper installation and testing of software modifications.

There are significant advantages associated with the availability of real-time assessments of fleet combat system readiness and capabilities. Real time and relatively continuous monitoring of combat systems' health status provides command personnel with an improved situational awareness of fleet capabilities at any time. Analysis of collected data may allow predictive maintenance actions, thus improving combat system availability and assisting in logistics and maintenance facility scheduling. These kinds of advantages allow command personnel to better utilize fleet assets and to maintain a higher percentage of combat systems availability.

The system architecture this capstone project develops results in a SWEF-Hub that provides many improvements in the maintenance and repair capabilities offered to the warfighters by the combat systems support groups as well as a centralized communication and data processing node. The development of the SWEF-Hub architecture, the main deliverable of this capstone project, identifies the technologies needed in order to provide the distance support in both the near-term and of the future, with the technologies becoming available over a ten-year timespan as they reach a state of maturity allows their use in a real-world USN setting.

B. TECHNICAL APPROACH

This SWEF-Hub capstone project develops a system architecture for the proposed SWEF-Hub. The technical approach used for the systems engineering (SE) process leads to the system architecture necessary to develop the SWEF-Hub over a ten-year development phase.

1. Systems Engineering Methods

The SE plan for the SWEF-Hub capstone project follows the Vee Model methodologies. The Vee Model is commonly used across the Department of Defense (DOD). Due to time constraints and the level of complexity of the task, the SWEF-Hub team executes only the technical design processes on the left side of the SE Vee Model shown in Figure 1. The left side of the Vee Model, tailored to the SWEF-Hub, allows progress to be traced from left to right. During the development of the system, the relevant systems engineering activities are defined and decomposed.

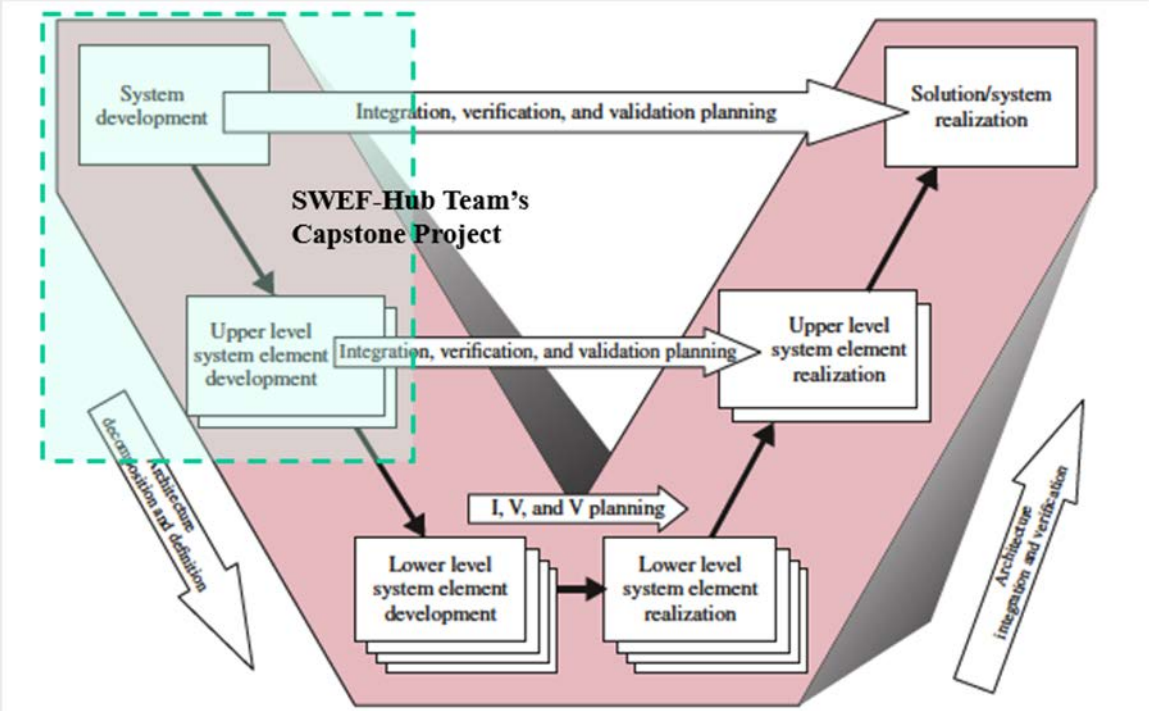


FIGURE 3.6 Vee model. Derived from Forsberg et al. (2005), Figure 7.10. Reprinted with permission from Kevin Forsberg. All other rights reserved.

Figure 1. Vee Model. Adapted from INCOSE (2015).

The primary reference document used during the SE planning and execution is the International Council of Systems Engineering (INCOSE) *Systems Engineering Handbook* (2015). The capstone team executes and analyzes four technical processes within the capstone project timeframe. The processes include mission analysis, stakeholder needs and requirements, system requirements definition, and architecture definition. Use of the Innoslate software program ensures traceability from initial stakeholder requirements throughout the technical processes.

Figure 2 displays a top-level breakdown of these four technical processes. It points to some of the inputs, activities and expected outputs associated with each process. The team accepts feedback from the stakeholders at two In-Progress Review (IPR) events. If the stakeholder feedback falls within the project scope and is feasible within the project timeframe, the team will adjust the project execution. The feedback maintains the stakeholders' engagement with the project. At capstone completion, the team delivers a

well-defined architecture for the future of distance support using SWEF facilities as the main hub for data processing.

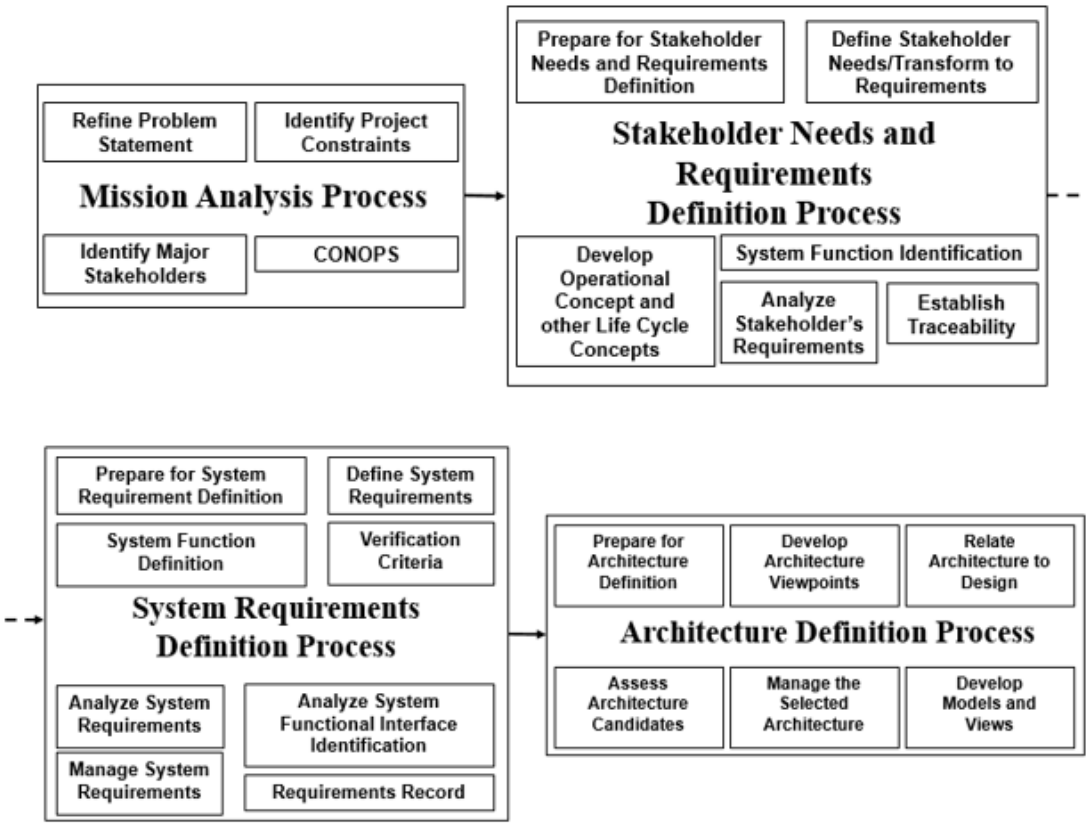


Figure 2. SWEF-Hub Tailored System Engineering Process

a. Mission Analysis Process

According to the INCOSE handbook, "the purpose of the Mission Analysis process is to define the problem, characterize the solution space, and determine potential solution classes that could address the problem" (INCOSE 2015, 49). The mission analysis process includes problem statement refinement, identification of stakeholders, and identification of the project assumptions and constraints.

Refinement of the problem statement occurs with input of the project visionaries and advice from the project advisors. The team generates a sound problem statement that

guides the development of the capstone project effort and ensures that the project visionaries (primary stakeholders) concur with the expected deliverables.

The project team identifies all major stakeholders and develops a concept of operations (ConOps) to describe the overall operation of the SWEF-Hub. The ConOps is a high-altitude picture of the system of interest. The preliminary ConOps captures the interactions of the system of interest (SOI) with other relevant organizations critical for mission success. The ConOps defines the initially identified boundaries of the system.

The team identifies both the presumptions inherent in the project and the known constraints affecting it. Mission analysis leads to the process of working with the stakeholders, and eventually leads toward the system functional architecture.

b. Stakeholder Needs and Requirements Process

The INCOSE handbook states that "the purpose of the Stakeholder Needs and Requirements Definition process is to define the stakeholder requirements for a system that can provide the capabilities needed by users and other stakeholders in a defined environment" (INCOSE 2015, 52). The stakeholder needs and requirements process includes preparation for the definition process, the development of operational concepts (OpsCon), and the development of measures of effectiveness (MOE).

The team prepares for the stakeholder needs and requirements definition. The team elicits the stakeholder needs from the participating identified stakeholders, then refines and transforms them into prioritized stakeholder requirements.

The team develops the OpsCon and considers other Life Cycle Concepts. In accordance with INCOSE, an OpsCon describes how the system works from the operators' perspective; it delves into the operational environment. It is a lower level view of the system. This step includes identification of the expected set of operational scenarios and the capabilities required for the SWEF-Hub.

From the stakeholder requirements and OpsCon considerations flow the identification of the functional requirements and the development of a functional hierarchy. Achievable MOEs are established. The team sets up processes that ensure traceability all

the way from the identified stakeholder needs down to the functional architecture elements. This effort leads to the system requirements definition process.

c. System Requirements Definition Process

In the INCOSE handbook, the authors state: "the purpose of the System Requirements Definition process is to transform the stakeholder, user-oriented view of desired capabilities into a technical view of a solution that meets the operational needs of the user" (INCOSE 2015, 57). The system requirements definition process includes preparation for the system requirement definition and the development of measures of performance (MOP).

The team prepares for system requirement definition by developing a sound understanding of the stakeholders' needs and the concept of operations. System requirement definition involves the identification of critical quality characteristics relevant to the system. The team identifies system functions in a solution-independent process. Pairing of stakeholder requirements with system requirements ensures traceability, and requirements records are established. Development of MOPs ensure the system requirements are satisfied. This process leads to the architecture definition process.

d. Architecture Definition Process

According to the INCOSE handbook: "the purpose of the Architecture Definition process is to generate system architecture alternatives, to select one or more alternative(s) that frame stakeholder concerns and meet system requirements, and to express this in a set of consistent views" (INCOSE 2015, 64). The architecture definition process includes the development of architectural viewpoints, models, and definition of interfaces.

The team identifies necessary technical, business, and operational information that allows the development of architectural viewpoints. Development of models and views describe interactions of the system entities with one another and define the system interfaces. The interfaces between the architectural elements are defined in order to ensure that the data elements necessary for the system to work are available. The team assesses the identified architectural candidates using system analysis and risk analysis processes.

2. Team Structure

The structural setup of the SWEF-Hub team separated participants into major functional areas as graphically shown in Figure 3. The structure assigns a primary and an alternate team member to each function in order to ensure project continuity in case of member absence due to required work travel or other uncontrollable events. The team consists of four roles as shown in Figure 3, each divided into a primary team member and backup team member(s). The team roles consist of project manager, system engineer, system architect, and technical editor. Additionally, each team member will fill in other roles when necessary. For the functions of system engineer and system architecture, the team assigned multiple primary members due to the expected workload.

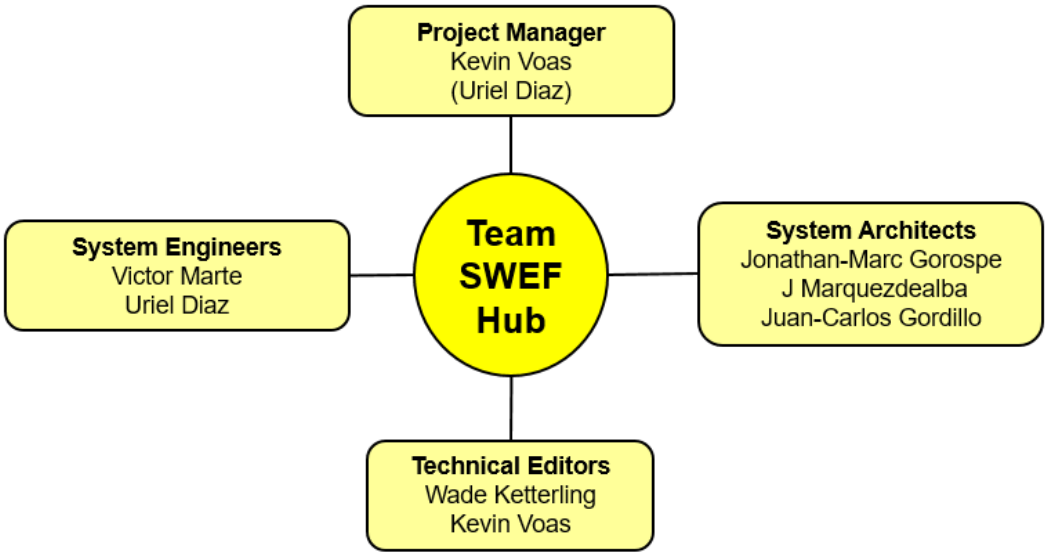


Figure 3. Team Organizational Structure

a. Project Participants

Each team member performs his assigned functions. The members also contribute to the other functional areas when their expertise, interests, or the needs of the project require it. Table 1 correlates the functional area to the assigned team members.

Table 1. Team Member Assignments

Functional Area	Primary Team Member	Alternate Team Member
Project Manager	Kevin Voas	Uriel Diaz
System Engineer	Victor Marte	
	Uriel Diaz	
System Architecture	Jonathan-Marc Gorospe	
	J Refugio Marquez De Alba	
	Juan-Carlos Gordillo	
Technical Editor	Wade Ketterling	Kevin Voas

b. Functional Role Descriptions

The project manager maintains the team structure, creates the project schedule, chairs meetings, and ensures that tasks are accomplished.

System engineers perform system design, development, and analysis. To perform these functions, the system engineer guides the evolution of the system through a system engineering process while managing complexity and risk.

System architects perform the design of system interface processes between people and technology.

Technical editors ensure that all presentations and reports follow the required formats, include technical content appropriate for a graduate-level report, and are free of errors.

C. BENEFITS OF STUDY

The Navy's leadership at Port Hueneme desires to modernize the combat system distance support to the fleet and move from the current process to a sophisticated, more efficient, and more secure process. The current communication process only allows the safe transfer and receipt of text messages (chatting), telephone calls, and emails from different locations. In order to fix a software or a hardware problem, ISEA personnel must

travel to the ship to troubleshoot and resolve the casualty. If a part is required but is not available on board the ship, it is requested and received after a casualty is observed; this has the potential of placing combat systems out of commission for an unacceptable period of time. To make matters worse, data extracted from the combat system having problems is packaged and mailed to a system support location for analysis, evaluation, and troubleshooting before the crew can receive recommendations; this process takes time. For all these reasons, it is important to provide the warfighter with the sophisticated tools needed to perform effective preventative and corrective maintenance to their combat systems through SWEF-Hub 24/7 distance support. The idea behind the modernization effort is to reduce or eliminate the downtime of combat systems so that they are ready when needed.

The new process and technology will allow a continuous monitoring of the combat systems' health and status to assist in predicting and preventing undesirable future events. Through the application of predictive analytics, information may be used to detect future combat system casualties before they happen, generating a preventive maintenance action to keep the system operating and thus reducing the system's downtime. Implementation of machine learning (ML) to accelerate and ease the analysis and interpretation of data extracted from combat systems assists the SWEF-Hub personnel in their efforts to provide immediate assistance to the fleet. In addition to that, it will be possible to provide software modifications and troubleshoot in real time. As for those situations where face-to-face distance support is required, utilization of audio and video facilitates the support process. For this effort, high data rates will be essential and implemented. New and sophisticated technology and processes implemented via the SWEF-Hub will benefit the Navy more than the current SWEF technology and processes; however, a higher level of cyber security protection will be required.

In the future, the distance support process will utilize sophisticated technologies for receiving data and information in real time at the hub. Centralized distance support for the United States Navy is one of the many goals of this plan. This will serve to increase readiness across the fleet and reduce support costs through centralization efforts. Once the SWEF-Hub is operational, the fleet will have better customer service because data and

information will be centrally routed through the SWEF-Hub rather than through many different locations as it is currently handled. Currently, data is not transferred in real time from a ship to the corresponding support facility. It takes a significant amount of time before the fleet gets a response with recommendations for resolving problems. The SWEF-Hub will continuously receive, analyze, and interpret data in order to evaluate the condition of combat systems. This helps to provide advance situational awareness, logistics support, and preventive and corrective recommendations in order to reduce or avoid future combat system casualties. If the SWEF-Hub does not have enough capability to analyze data, then any data captured and information obtained in previous analysis will transfer to a secondary location for further analysis. In summary, the data transfer and analysis process will be faster, and the response time will be shorter. In turn, this will reduce the downtime of combat systems. In a situation where a potential system problem is not identified in advance and a combat system casualty occurs, further steps will be taken.

If a serious problem arises that was not detected by the data analysis process and the ship's force is not able to solve it, secured distance troubleshooting in real time from the SWEF-Hub will be implemented in order to trace software and hardware-related issues and to resolve the problem. For problems that require some physical involvement on the ship to troubleshoot the combat systems, the experts at the hub will collaborate with the ship's force by utilizing audio and video to guide them in the implementation of the troubleshooting process. This will reduce the need for on-site field engineers for combat system support. Furthermore, periodic distance troubleshooting will assist in the discovery and correction of cybersecurity vulnerabilities through software modifications.

To improve the performance and security of combat systems, the SWEF-Hub will provide a secure connection for software updates, upgrades, and repairs. If a ML system were part of a ship's systems, it would carry out some of the functionality associated with the SWEF-Hub for system analysis, maintenance, and troubleshooting. It would work with the SWEF-Hub in an abbreviated way. The more often the ML system on a ship receives updates and upgrades with information provided through the SWEF-Hub, the more independent that Navy ship will be in preventing and resolving problems.

The main goals behind this project are to provide NSWC PHD with the means to improve and facilitate combat system distance support, to reduce the downtime of combat systems around the fleet, and to make ships more independent in the future.

D. DESCRIPTION OF CHAPTERS

This section describes the purposes of the following chapters of the capstone project.

Chapter II focuses on the mission analysis process. The project's problem statement and vision are refined. Current distance support capability is assessed. Concepts of operations are developed, and major stakeholders are identified. Project scope, assumptions, and constraints are considered.

Chapter III focuses on the stakeholders' needs and requirements definition process. Stakeholder needs are transformed into requirements and detailed operational concepts are developed. Stakeholder requirements are analyzed, and traceability is established.

Chapter IV focuses on the system requirements definition, building upon the mission analysis and stakeholder requirements necessary to construct the architecture definition process.

Chapter V focuses on the system architecture and covers the functional, physical, and interface architectures. In every step of the architecture definition process, each defined architecture provides a structure that helps to define the following architecture. The SWEF-Hub architecture was conceptualized in two timeframes, near-term and long-term. The near-term architecture provides the initial concept. The long-term architecture builds upon the near-term architecture for its realization.

Chapter VI presents the conclusions for the application and implementation of the selected system architectures that were developed, as well as recommendations for further research.

THIS PAGE INTENTIONALLY LEFT BLANK

II. MISSION ANALYSIS PROCESS

The systems engineering mission analysis process defines the statement of need and the scope of the project. Naval Surface Warfare Center Port Hueneme utilizes a distance support capability to provide technical support to increasingly advanced combat systems in the fleet. This capstone provides an architecture for a distance support capability that encompasses new and upcoming technological advances to support an increase in operational availability and reduce duplication of efforts across the NAVSEA enterprise. This chapter provides the basis required to identify and describe the stakeholder requirements that will be formally proposed in Chapter III, as well as the system scope necessary to complete the system analysis in Chapters IV and V. Figure 4 represents the customized SE mission analysis process used by the SWEF-Hub capstone team.

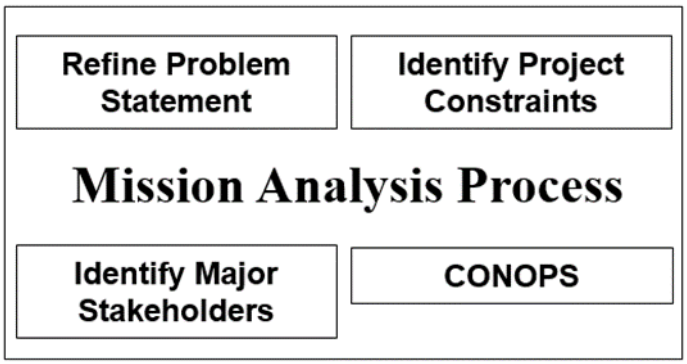


Figure 4. Customized SWEF-Hub SE Mission Analysis Process

"As stated in ISO/IEC/IEEE 15288, the purpose of the Business or Mission Analysis process is to define the business or mission problem or opportunity, characterize the solution space and determine potential solution class(s) that could address a problem or take advantage of an opportunity" (INCOSE 2015, 49). The mission analysis process diagram shown in Figure 4 has four steps. These include refining the problem statement, identifying the major stakeholders, developing a concept of operations, and identifying any project constraints. Team SWEF-Hub has met with the primary stakeholders, considered

the visionaries of the project, as well as with the project advisors in order to develop a sound problem statement; the problem statement helps with the development of the project and promotes following the requirements of the visionaries. The team identified all major stakeholders in order to use their requirements to develop a concept of operations. The mission analysis process is an iterative process, and as the process continues, project constraints are identified, resolved, or mitigated.

Figure 5 shows the inputs used in the mission analysis process, the process activities, and the outputs that result from the process.

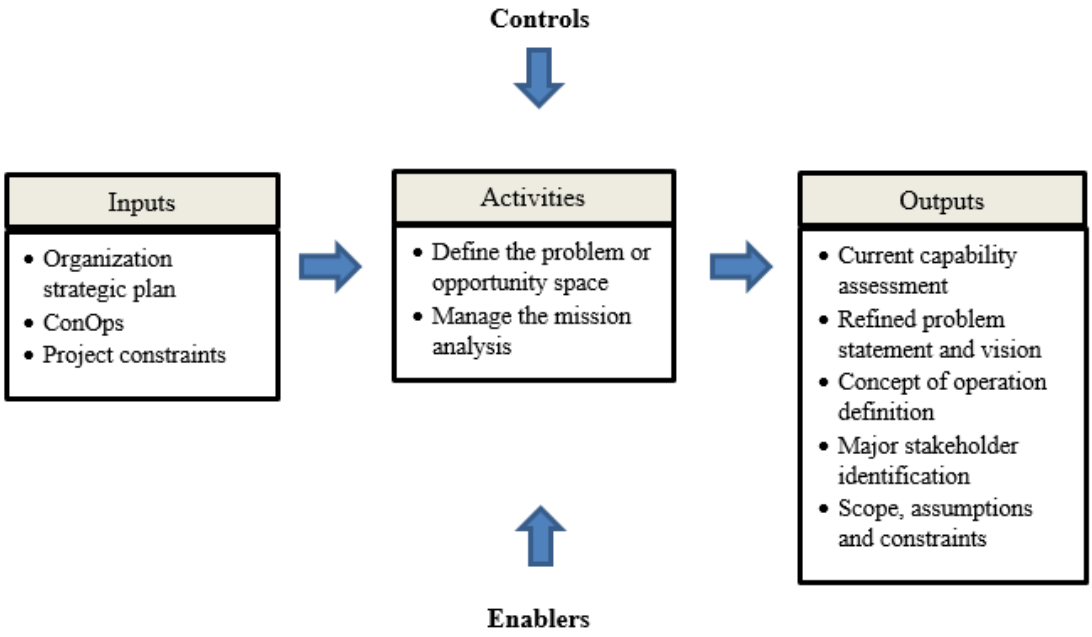
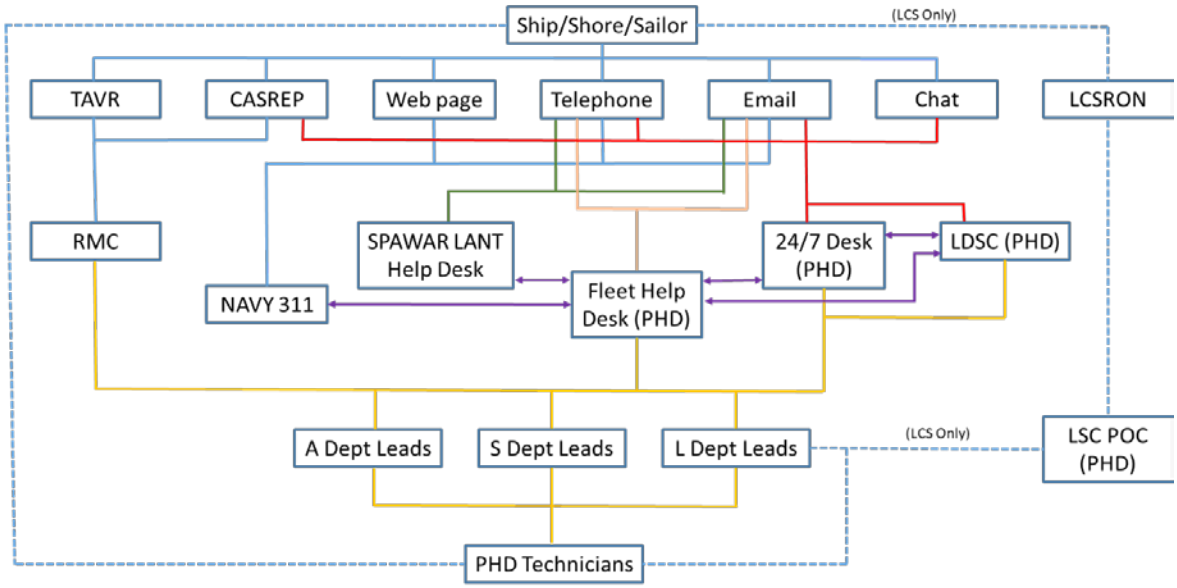


Figure 5. Mission Analysis Input-Activity-Output Diagram. Adapted from INCOSE (2015).

A. CURRENT CAPABILITY ASSESSMENT

NSWC PHD's existing capability to provide distance support (DS) resides in three dedicated support centers providing redundant and overlapping activities (stove piping). A single ship class designated routing for LCS, a documentation website, and subject matter expert (SME) direct assistance center. Figure 6 is a visual representation of NSWC PHD's current process, with the color-coding serving to assist in visually separating the lines. It

shows the numerous entities within NSWC PHD who work together to provide distance support for combat systems equipment, as well as several entities with whom NSWC PHD routinely liaisons in the performance of the distance support function. This process is, at best, difficult to follow and understand. As new DS capabilities were introduced into the overall support organization, they were allowed to retain their original focus as developed by their program sponsors; the result is a noticeable lack of a single-entry point into the NSWC PHD distance support architecture.



Colored lines are used to visually separate flow processes

Figure 6. NSWC PHD Current Process

1. NSWC PHD Distance Support Centers

The three distant support centers are the Aegis Technical Team (AegisTT), the Littoral & Strike Warfare Distance Support Center (LDSC), and the Fleet Help Desk.

PHD's AegisTT operates on a 24-hour, 7-days-a-week (24/7) support rotation. In addition to supporting the Aegis Combat Systems in the fleet, the support center receives fleet requests for assistance to support the PHD Expeditionary Warfare Department. Information comes from the fleet sailor through telephone communications and web services such as email and chat rooms as shown in Figure 7, as well as casualty report (CASREP) message traffic as shown in Figure 8.

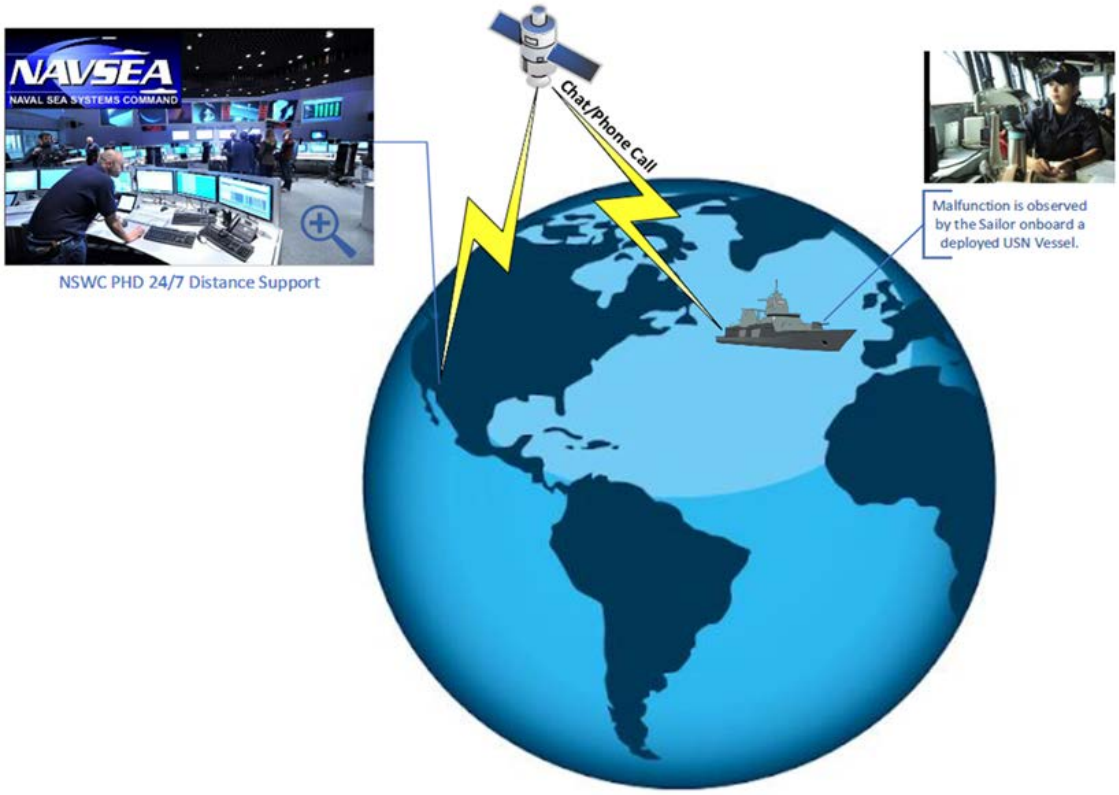


Figure compiled using Lucidchart, accessed July 2019, www.lucidchart.com.

Figure 7. Technical Assistance Requested via 24/7 Distance Support (NSWC PHD)

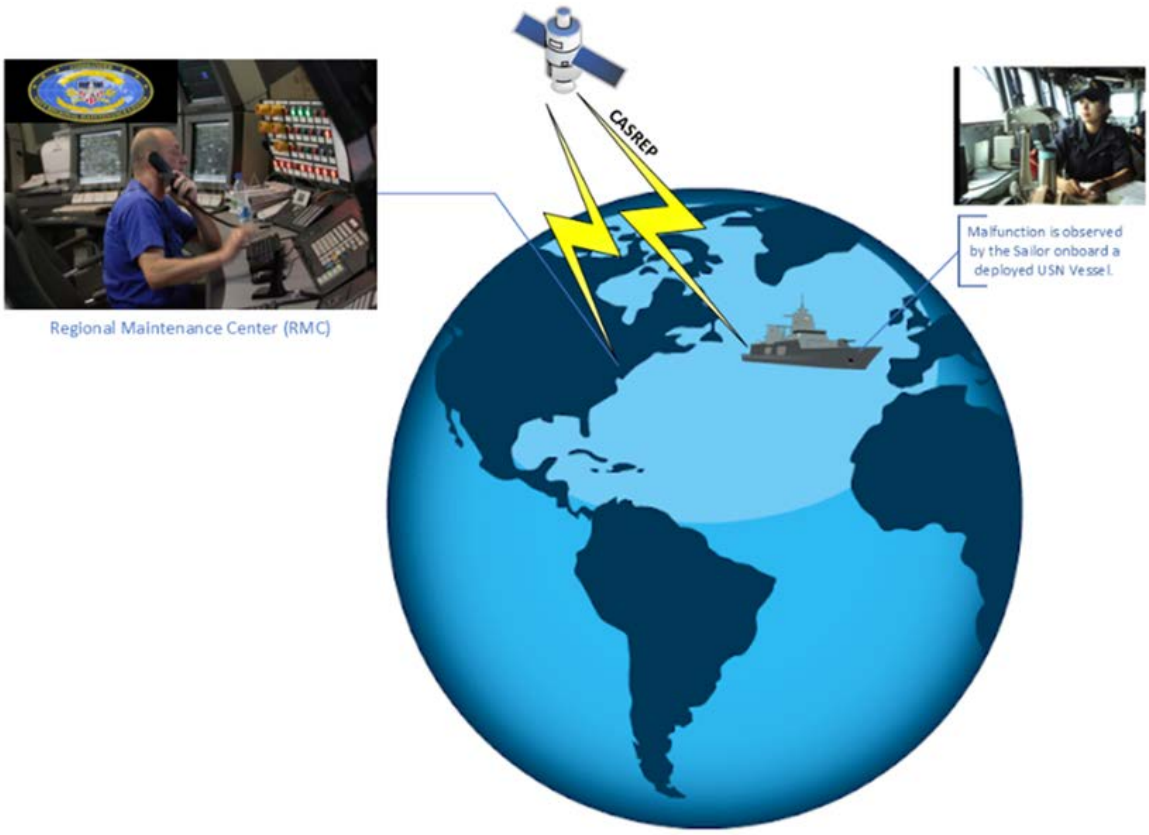


Figure compiled using Lucidchart, accessed July 2019, www.lucidchart.com.

Figure 8. Technical Assistance Requested via Casualty Report (CASREP)

AegisTT is equipped to receive, process, and store both unclassified and classified information. The watchstanders within the AegisTT record the information and route requests to PHD SMEs for resolution. The routing system is an electronic ticketing form and documentation system built upon the Global Distance Support Center (GDSC) format (explained below). The routing used to reach the PHD SMEs is based upon which combat systems equipment the message concerns. SMEs receive notifications and assistance requests via email or telephone. There is typically a time delay between receipt of the assistance request at PHD and action by the requisite SME; SME positions are not staffed 24/7. In the instance of a critical request, the AegisTT watch stander has the capability to recall a SME in order to provide immediate assistance; that goal is not always achievable.

Limited numbers of SME personnel and the need to travel to distant facilities to troubleshoot complex systems sometimes results in the non-availability of an SME.

PHD's LDSC operates as a fully manned distance support center only during normal working hours (Pacific Daylight Time). It receives funding to operate for major fleet exercises or for real-world support (when authorized). When the LDSC is performing support operations, it functions similarly to the AegisTT center.

PHD's Fleet Help Desk operates as a telephone call center to provide service from the fleet to different SME departments. Additionally, the Fleet Help Desk is the primary hub between GDSC and PHD departments. Due to the nature of combat systems and support equipment, SPAWAR (now designated Naval Information Warfare Center (NIWC)) also receives requests for assistance. Due to the complexity of equipment communications, the Fleet Help Desk acts as the liaison between NIWC and NSWC PHD. The Fleet Help Desk is also the focal point to maintain NAVSEA's information website Sailor-to-Engineer (S2E).

The Littoral Combat Ship Squadron (LCSRON) maintains a link between their hulls and the technical community at NSWC PHD. Fleet technical assistance requests originate at the hull level because a Littoral Combat Ship (LCS) rotates crews on a regular basis. LCSRON receives the assistance requests from the LCS, then directly contacts NSWC PHD LCS SMEs for resolution. The NSWC PHD LCS SME independently works the issue to completion without other NSWC PHD DS support systems. However, in some cases, an LCS sailor contacts the GDSC which then generates a ticket routed via the NSWC PHD Fleet Help Desk and then to the NSWC PHD LCS SMEs.

2. NSWC PHD SME Support

An indirect route for technical assistance, consisting of direct contact between the fleet sailor and the SME for the requisite equipment, is sometimes used. Sailors often acquire technician contact information. The sailor often considers contacting the SME directly to be the quickest, least cumbersome path to achieving equipment restoration. This type of contact is not discouraged; however, the results are not consistently documented. Documentation is necessary for historical, logistical, and analytical purposes. Without this

data, the technical support centers lose system performance data, miss trends in maintenance metrics on fleet elements, lose track of maintenance and troubleshooting hours spent, and miss logistics requirement changes. Overall, the system support organization fails to capture necessary and highly valuable information.

3. Test and Evaluation (T&E)

Testing and evaluation for shipboard systems occurs on a regular basis, whether testing new capabilities, verifying and validating equipment installations, or performing shipboard system qualifications as shown in Figure 9. The NSWC PHD T&E branches capture data from these events and store it for analysis by NSWC Corona Division.

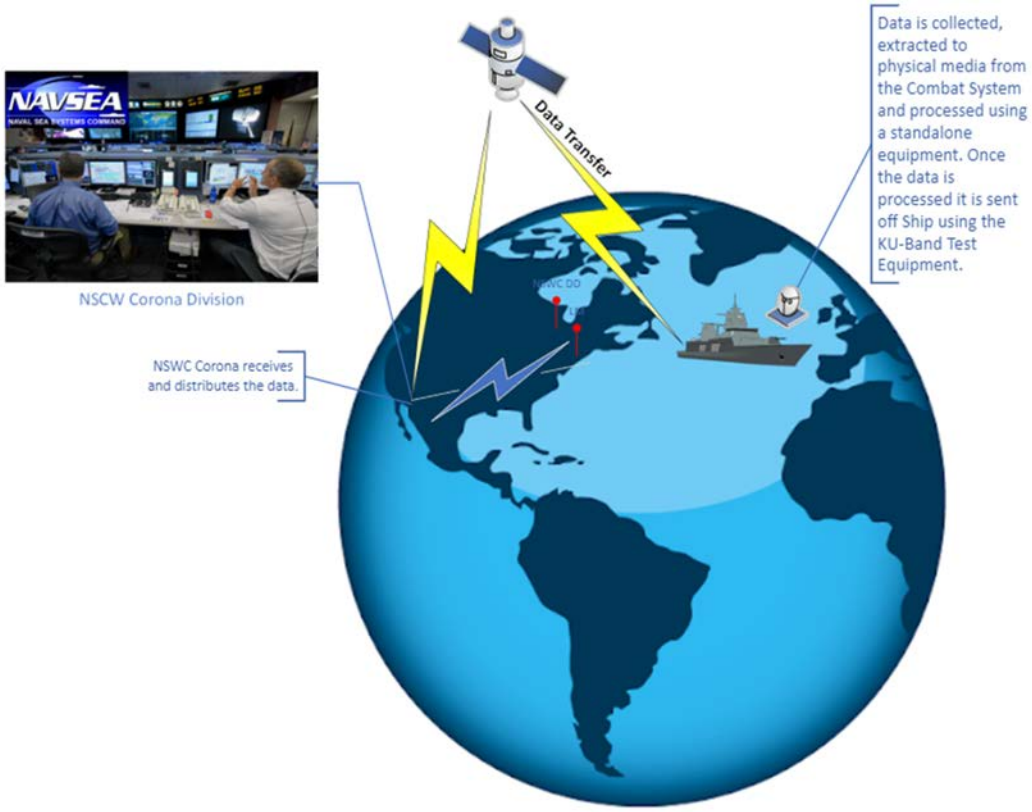


Figure compiled using Lucidchart, accessed July 2019, www.lucidchart.com.

Figure 9. Test and Evaluation (T&E)

4. NAVSEA Support

The Naval Sea Systems Command documentation website is entitled Sailor to Engineer (S2E). NAVSEA's S2E website provides technical documentation, point-of-contact listings, equipment assistance, assistance documents, support links, advisory messages, newsletters, and support requests on both classified and unclassified systems. This is a repository of system or equipment information and is updated and maintained often at a technician level. Any Department of the Navy (DON) member can acquire a S2E account and log into the system for information.

5. Navy Support

As background information, it is important to know that the USN, as a whole, operates a centralized information hub operated as NAVY 311. This hub is located in New Orleans, LA, and responds to calls from all elements of the Navy for distribution out based on the information requested. PHD is a component of the NAVY 311 system as a Global Distance Support Center (GDSC) participant. NAVY 311 fields all types of information requests through web-based services via chat, email, web forms, websites, and telephone calls. NAVY 311 is not structured to receive direct digital equipment data as envisioned for the SWEF-Hub, nor is NAVY 311 set up to handle classified information. The GDSC holds the digital "ticket" format data in a database entitled "Remedy." The Remedy database is the ticket hub and operates as the distribution center to numerous USN activities, not just NAVSEA. These activities include but are not limited to NAVSEA, NIWC, Naval Installations Command (NIC), NAVMED (BUMED), and BUPERS (Bureau of Personnel). NSWC PHD also uses the digital ticket format to capture fleet issues and the path to resolution. Maintaining the ticketing system allows tracking of each issue to completion as well as the generation of a historical database of issues. Attempts to automate the system are progressing; however, the system currently requires manual data input and cannot receive the type and volume of system data that the SWEF-Hub will require.

B. REFINED PROBLEM STATEMENT AND VISION

The Naval Surface Warfare Center Port Hueneme Division (NSWC PHD) requires a redesign of the Surface Warfare Engineering Facility (SWEF) to act as a central hub for future real-time Navy combat systems distance support. This SWEF-Hub will employ advanced technological concepts to assist the warfighter to perform effective and timely preventative and corrective maintenance to their equipment. The hub will furnish NSWC PHD with the tools necessary to reduce the need to field on-site field engineers while providing the health status of combat systems on every ship to the departments within NSWC PHD. The SWEF-Hub will incorporate a means to collaborate in real time with the U.S. Navy's leadership and fleet sailors to streamline decision-making processes. The goal of the SWEF-Hub redesign is to provide a more efficient use of support resources that will result in increased productivity of the maintenance and support personnel, increased situational awareness concerning the status of combat systems, and improved customer service to the warfighter.

In accordance with the project's primary stakeholder, NSWC PHD, the vision for the SWEF-Hub project is as follows:

> A technologically advanced Surface Warfare Engineering Facility hub that effectively integrates real-time combat system ISEA distance support to fleet elements, provides real-time combat systems status data from fleet elements, and provides a feedback path to and from command elements.

The context diagram displayed in Figure 10 is a graphical representation of the internal functions of the SWEF-Hub, the hub's functional interfaces, and the external entities it services.

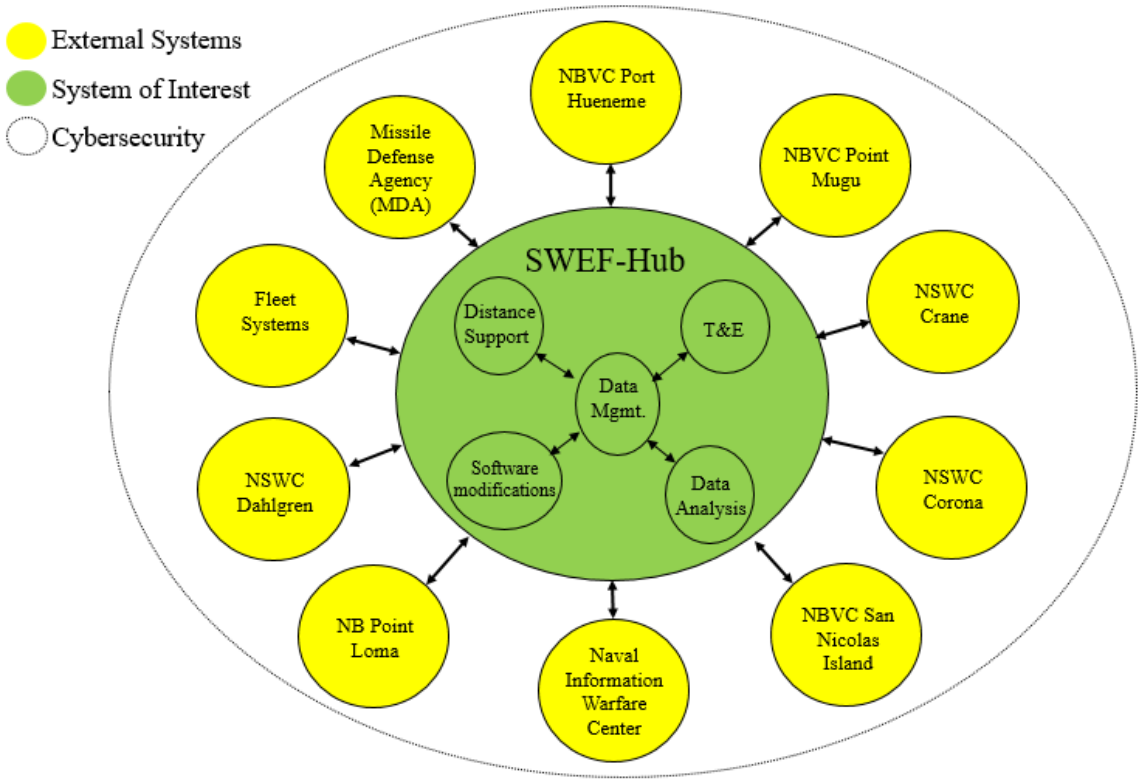


Figure 10. SWEF-Hub Context Diagram

In accordance with the sponsors' vision, the project team intends to use SE processes to develop a system architecture suitable for the SWEF-Hub. When implemented, the SWEF-Hub will employ the most advanced technological concepts available considered mature enough for incorporation. The hub will allow real-time distance support for the surface combatants from the various combat system In-Service Engineering Agents (ISEA) entities located at NSWC PHD and other NSWC locations. The SWEF-Hub will provide a path and a toolset that allows secure system software updates, monitoring of combat system(s) status and data analysis, predictive system analysis, and real-time assistance for maintenance, testing, and repair of combat systems. In addition, the hub will provide a channel for command(s) to monitor fleet combat system status and communicate related directives to the fleet elements.

C. CONCEPT OF OPERATION DEFINITION

As part of the concept of operations definition and as illustrated in Figure 11, the SWEF-Hub Capstone project team has identified the basic interfaces necessary to address stakeholder needs, as well as the boundaries that will enable effective and reliable distance support from NSWC PHD. The operational concept of the SWEF-Hub captures the features, connections, and technologies required to provide distance support for the fleet, independent of geographical location and environmental conditions. The goal of using SWEF facilities as the central hub for naval distance support includes increasing readiness, system up time, and Navy wide situational awareness.

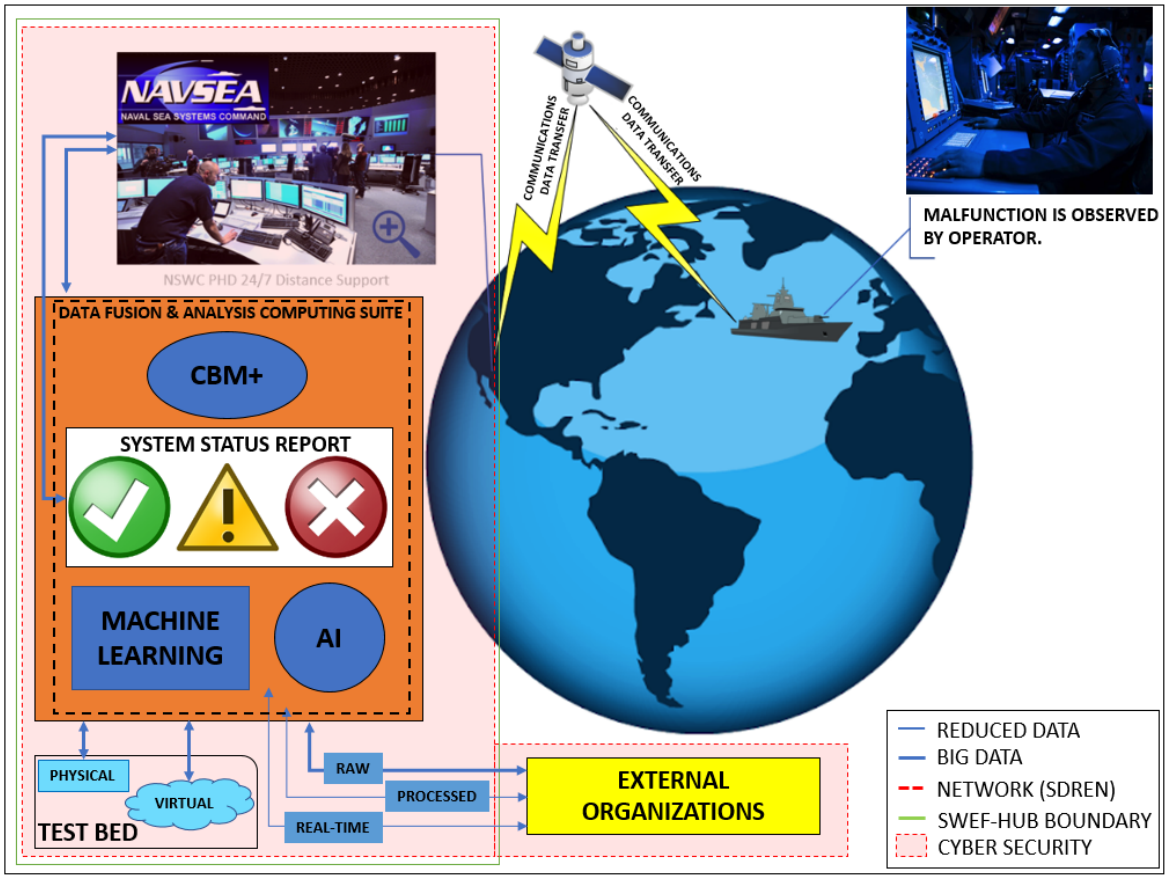


Figure compiled using Lucidchart, accessed July 2019, www.lucidchart.com.

Figure 11. SWEF-Hub Operational Concept

1. SWEF-Hub Operations

Multiple entities will leverage from the SWEF-Hub as envisioned, with the fleet as the primary beneficiary. The operation of the SWEF-Hub requires a collaborative effort guided by human interaction, especially considering that the distance support center will operate 24/7.

a. Watchstanders

The SWEF-Hub concept provides a platform for operators with different levels of expertise to collect, quickly and precisely, the information necessary in order to provide a problem resolution within improved turnaround times. The intent of the SWEF-Hub architecture as envisioned is for technicians with entry to journeyman level expertise to operate the hub workstations under the guidance of at least one senior (lead) level technician or engineer on every watch. Problems will be categorized, then the watchstanders will try to provide an accurate response using in-house technical resources and historical data. If the watchstander is unable to resolve the problem within a given timeframe (time value to be provided by the stakeholders), the problem will be elevated so an SME's attention is brought to bear on the issue.

b. Subject Matter Experts (SME)

The identification of critical element SME and point of contacts (POCs) will be part of the infrastructure of the SWEF-Hub. Until several technologies such as machine learning and artificial intelligence (AI) reach an acceptable level of technology maturation and reliability, human judgement and expertise will be the critical component of the SWEF-Hub operation. Watchstanders will have multiple methods of communication in order to reach out to the SME when necessary. SMEs will adhere to command procedures and comply with security regulations to ensure mission integrity.

2. External Organizations

Inputs from certain external organizations are required in order to accomplish effective and thorough distance support for various combat systems. External organizations will need to comply with minimum equipment configuration requirements to enable the

capability to securely send and receive information. Once the interface is established, the SWEF-Hub will be able to share near real-time ship health status as well as raw and processed data with those entities having the capability to analyze the data and provide valuable inputs. After performing a complete assessment on deployed capabilities across USN assets, the following organizations and their external interactions have been identified as essential interfaces in order to increase the supportability of the fleet.

a. Fleet Combat Systems

Contact with fleet sailors supporting combat systems is a critical interaction. The effectiveness of the SWEF-Hub distance support center will be dependent on how effectively and expeditiously it can exchange information with deployed USN assets.

b. NSWC Crane

NSWC Crane supports electronic warfare (EW) elements such as the AN/SLQ-32. Effective and available communication channels between NSWC Crane and the SWEF-Hub is essential to support multiple EW elements expeditiously.

c. NSWC Corona

NSWC Corona serves as the main data storage (physical and digital) site for the Aegis community. NSWC Corona has a wide range of experienced, full-time data analysts. The SWEF-Hub's ability to communicate and share information with NSWC Corona will provide redundancy for data analysis and storage; their expertise and availability will be essential for mission success.

d. Naval Information Warfare Center (NIWC) Pacific

NIWC Pacific develops and supports Tactical Data Links currently deployed across the fleet; a lot of what our Navy is capable of doing today would not be possible without them. The interaction between the SWEF-Hub and NIWC will be important to keep our links operational and ready to support the mission.

e. NSWC Dahlgren

NSWC Dahlgren is responsible for certifying Combat System baselines prior to their official deployment to the fleet. Additionally, they provide software analysis for various combat systems. Involving NSWC Dahlgren in distance support efforts will assist in the development of future software upgrades and in generating new developments.

f. Missile Defense Agency (MDA)

MDA is the main funding source for the Ballistic Missile Defense (BMD) capability onboard guided-missile cruisers (CG), guided-missile destroyers (DDG) and Aegis Ashore (AA) sites. MDA should be involved in the sharing of data/information of any issues related to BMD. The involvement of MDA in early on troubleshooting efforts and the identification of existing system problems could enable MDA to start driving fixes for future upgrades and software development efforts. Having the expertise locally at NSWC PHD to support BMD systems onboard Navy vessels could also serve as justification for receiving additional funding from MDA.

g. Naval Base Ventura County (NBVC) Point Mugu

New Directed Energy (DE) capability is currently under development. The new Directed Energy System Integrated Laboratory (DESIL) facility in NBVC Point Mugu will maintain these new systems. Currently, LPDs, DDGs, and LCS are the hulls under consideration to field the DE systems. It is important to take advantage of existing and relevant future capabilities that will have a direct connection to and interactions with new DS systems by establishing the appropriate infrastructure. This will include connections to combat systems already present at SWEF.

h. NBVC San Nicolas Island

Telemetry for nearby naval exercise test events is currently collected at NBVC San Nicolas Island. Integrating this data into the SWEF-Hub infrastructure will provide an enhanced capability. This will allow near real-time data transfer from test events into the applicable SWEF-Hub laboratories and improvements in the response time for accomplishing data analysis.

i. NB Point Loma

A large amount of fleet operational data passes through a collection point at NIWC Complex Point Loma. Leveraging this data would provide improved situational awareness both to the SWEF-Hub and to NIWC Point Loma.

j. NSWC PHD

In addition to the SWEF building itself, NSWC PHD has multiple independent buildings that support different platforms across the Navy. The ability to exchange information within NSWC PHD across the command (e.g., the LCS Mission Package Support Facility (MPSF)) will facilitate a quicker response time associated with the review, analysis, and problem resolution anytime assistance requests route through the SWEF-Hub.

3. SWEF-Hub Data Fusion and Analysis Capability

The effectiveness of the SWEF-Hub will relate to how quickly, accurately and securely it can receive, send, and process information (data). The SWEF-Hub will leverage from currently deployed capabilities, as well as future planned technologies in order to provide accurate and timely problem resolutions.

a. Network (SDREN)

During the team's meetings with Stakeholders, NSWC PHD command elements very specifically stated the importance of developing a system that complies with PHD's requirements for Information Technology (IT) equipment that will be connected to the core networks in accordance with OPNAV 5239.2A. More specifically, those networks used for classified information (i.e., SIPR, SDREN etc.) must meet security requirements.

b. Cyber Security

Cyber security measures and equipment incorporated into the SWEF-Hub must "be consistent with Federal Information Security Management Act (FISMA), DOD and DON policies and guidance" (Department of the Navy [DON] 2017, 1).

c. Data Management

Data analysis will play a major role for the SWEF-Hub, arguably one of its single most important capabilities. The ability to constantly analyze data, identify problems hidden in that data, observe and document patterns, and then feed all of this information into the technologies listed above will be the factor that ensures combat system readiness across the fleet. The incorporation of advanced and predictive analytics methods, combined with Condition-Based Maintenance Plus (CBM+), will help to keep the fleet's systems operational for longer periods and extend the operational life of the systems.

d. Health and Status Monitoring Systems

Situational awareness is one of the most critical components for readiness. Having the ability to remotely monitor the status of fleet asset's combat systems and adjunct components will enable not only the SWEF-Hub operators to provide fault isolation recommendations but will also aid leadership in their decision-making processes. The direction for the SWEF-Hub includes the incorporation of advanced technologies that allow near-real-time status reports; this data will feed into a machine learning technology-based system where analysis will be accomplished. The ability of the SWEF-Hub operators and fleet sailors to share a common picture, viewing alerts and system indications, will allow the SWEF-Hub operators to engage in a collaborative effort to resolve issues.

e. Condition-Based Maintenance Plus (CBM+)

CBM+ will be among the major technologically advanced capabilities incorporated into the SWEF-Hub, allowing prediction of system failures before they occur. This capability has been among the major groundbreaking technologies to improve reliability in the aerospace and automotive industries. Some departments in NSWC PHD have begun incrementally testing similar capabilities. Data captured from issues encountered by both navy sailors and SWEF-Hub watchstanders will be stored, analyzed and maintained in the computing suites. This data, along with other sources of historical data (i.e., test event related and historical data), will undergo constant analysis in order to develop these equipment behavior patterns. The most common issues, identified and investigated through fleet data metrics, will serve the function of waypoints in the identification of potential

failures. The newly identified potential failures will be considered and mitigated in the newer systems.

f. Advanced Logistics

Identifying issues early will allow the SWEF-Hub watchstanders to send out alerts to different ships. Alerts will include valuable information about predicted potential failures, listing specific parts and components. This information will be sufficient for sailors to begin the acquisition process of these parts and by the time the parts fail, the replacement part will have arrived or be on its way. SWEF-Hub personnel could also assist the sailor with this process.

g. Software Modifications and Configuration Management

The main database at the SWEF-Hub will have up to date information on all combat related configuration management from a hardware and software perspective. Having this valuable information on hand will allow the watchstanders to narrow down search results to specific ship configurations when resolving issues. The information helps to identify affected ships after discovery of software problems, as well as assisting in the identification of alert recipients when new and/or upgraded software becomes available. The direct line of communication between the SWEF-Hub and deployed fleet assets will also facilitate the deployment of software upgrades; the operators can both notify and send upgrade packages to the ships and collaborate with the upgrade process.

In addition to combat system information, the SWEF-Hub will also support fielded cyber security tools already in use in the fleet, managed by NSWC PHD. These tools include (but are not limited to) Host Based Security System (HBSS) and Security Information and Event Management (SIEM) deployed software. Both tools provide significant cyber security for deployed systems in real time. By being able to push and pull data from deployed systems, the SWEF-Hub will provide a significant method for both proactively managing configuration on deployed systems and retrieving status for cyber security assessments. By being able to deploy new patches and/or software configurations based on new threats identified by Information Assurance Vulnerabilities Alerts (IAVA), TASKORD, OPORD, or new program office directions, the SWEF-Hub will reduce the

amount of time normally required to ship software to each deployed unit. Reports from those systems arrive at the SWEF-Hub for retrieval and analysis by the respective SME(s) for immediate support.

h. Virtual Twin (Physical) and/or Virtual Test Bed (VTB)

Among the benefits of purchasing a Virtual Twin (VTwin) computer suite to be configured with multiple Aegis baselines and operated from NSWC PHD, is the capability of providing efficient distant support for software centric issues. Initially, the VTwin will operate as a standalone system. The SWEF-Hub requires a high data-rate connection to the suite, where data can be continuously shared for event reconstruction. Results arrive back at the SWEF-Hub for further data analysis and investigation; the SWEF-Hub shares the findings with the fleet along with recommended solutions to address the problem. The VTwin will allow the supporting team to recreate numerous software malfunctions utilizing the same displays, Variable Action Buttons (VAB), and a system logic identical to shipboard configuration. From the same physical location in NSWC PHD, the same team will have the capability to remotely access a full shipboard representative Aegis suite, which would provide the best option for resolving hardware related problems.

D. MAJOR STAKEHOLDERS

Stakeholders are personnel directly affected by the SWEF-Hub project. NSWC PHD holds the vision for the SWEF-Hub project as well as the physical location for it. The SWEF-Hub team identifies them as the primary stakeholder. Table 2 lists the stakeholders. Secondary stakeholders are personnel (within the listed commands) directly affected by the SWEF-Hub capabilities investigated within this project. The fleet ships and Aegis Ashore facilities receive readiness capability; the Regional Maintenance Centers (RMCs) utilize information collected by the SWEF-Hub to direct repair efforts; Commander, Naval Surface Force (CNSF) realizes increased readiness on surface ships; NAVSEA is the direct reporting authority of NSWC PHD; and Program Executive Office (PEO) is the primary funding source.

Table 2. SWEF-Hub Stakeholders

	Stakeholder	Description	
1	NSWC PHD	Overall Command where facility will be located	Primary
2	PHD Code 203	NSWC PHD Lead System Engineer	Primary
3	A Department Manager	Air Dominance Department	Primary
4	L Department Manager	Littoral and Strike Warfare Department	Primary
5	S Department Manager	Ship Defense and Expeditionary Warfare Department	Primary
6	PHD Code 206	PHD Distance Support Customer Advocate	Primary
7	Fleet Ships/Aegis Ashore Facilities	Direct Customer of SWEF-Hub Capabilities	Secondary
8	Regional Maintenance Center (RMC)	Support Activity Benefiting from SWEF-Hub	Secondary
9	Surface Force Type Commander (CNSF)	Commander of Fleet Ships	Secondary
10	Naval Sea Systems Command (NAVSEA)	Command for Engineering, building, and supporting the fleet	Secondary
11	Program Executive Office (PEO)	Develops, delivers, and sustains operationally dominant combat systems	Secondary

The Aegis Ashore (AA) facilities perform a particularly unique specific mission of Ballistic Missile Defense (BMD) and utilize the Aegis system at its core. At the time of this report, there is one active AA facility in Romania, with other locations either under construction and/or planned. U.S. Navy personnel work at AA Romania and NSWC-PHD monitors it as part of Aegis support.

E. SCOPE, ASSUMPTIONS, AND CONSTRAINTS

In order to accomplish the SWEF-Hub architecture design over the course of a capstone project, the team set limits on the work products that it could produce in the form of a project scope. During the mission analysis process, it became clear from the visionary's statements that certain assumptions regarding the SWEF-Hub capabilities were required. In addition to the time limitations, constraints included a specified geographical location for the SWEF-Hub and unknowns regarding the funding process required to implement the project at some future point in time.

1. SWEF-Hub Project Scope

The SWEF-Hub capstone project develops a system architecture for the SWEF-Hub. The project visionaries intend to implement the SWEF-Hub in the near future, but intend for the technology portion of the implementation to include currently immature technologies that will be developed over the next decade. Funding planning concerning how each affected program that benefits from the SWEF-Hub implementation financially supports it is outside of the scope of the capstone project. Within the scope of the capstone project, the SWEF-Hub team will deliver the following work products:

- A system architecture
- A recommendation for further SWEF-Hub analysis

2. SWEF-Hub Project Assumptions

The capstone team makes assumptions concerning the capabilities that the SWEF-Hub must provide. These assumptions help to guide the team in the determination of the needs that the system must fulfill. They include the following:

- The SWEF-Hub will provide an interface between various shore-based elements and fleet elements. While not completely defined, it is assumed that the interface will allow the passage of numerous types and formats of data, multiple classification levels, and real-time data communications.

- The SWEF-Hub requires incorporation of IA and cyber security aspects in all its functional architecture elements. Making the SWEF-Hub a centralized interface point for combat systems support communications will potentially lead to a type of single-source failure point; however, it is assumed that applying IA and cyber security to a single hub will make the SWEF-Hub architecture a harder security target than a divided group of separate communications nodes.

- It is assumed that making the distance support capabilities consistent across multiple combat systems will be viewed as an improvement over the current distance support capabilities. It is a priority element in the system architecture design of the SWEF-Hub.

- The nature of the concept for the SWEF-Hub should work to improve the situational awareness of command personnel concerning the status of fleet combat systems. While not explicitly specified in the design, the user interfaces will be key to visualize and interact with situational information. It is assumed that the displays and user interfaces will be designer in a manner to present the necessary information and offer users the control needed to improve situational awareness.

- Interfaces on fleet assets will be recommended, but the implementation of those interfaces are beyond the scope of this project. The capstone team assumes that the fleet will implement the interfaces required to support interaction with the SWEF-Hub.

- The specific technologies that the SWEF-Hub implementation will use is beyond the scope of this capstone project; the stakeholders do not want the project to constrain itself to currently mature technologies. The requisite technologies will mature over the next decade and be available for use.

- The transition to the SWEF-Hub cannot preclude any current support operations. NSWC PHD must continue to support the functions of distance

support at all times; it is assumed that operations cannot be stopped during the implementation of the SWEF-Hub infrastructure. The ability to return to the original rendition of distance support capability must be maintained. This may force a duplication of effort and function until the SWEF-Hub infrastructure has been tested and proven to operate as expected.

3. SWEF-Hub Project Constraints

The SWEF-Hub project team is constrained by both factors of available time and limitations set forth by the project visionaries. The scope of the SWEF-Hub capstone project resides within the following constraints.

- Time: A large amount of effort goes into the development of a distance support center. The limited amount of time available for the team to develop this architecture is a constraint. The time constraint limits the level of detail that the team provides during the study, as well as the depth of the investigation.

- Geographical Location: The scope of the project does not include determining the location of the distance support center. NSWC PHD has clearly stated that they want the distance support center to be located at NSWC PHD. More specifically, they want to locate it at the Surface Warfare Engineering Facility (SWEF); hence, SWEF-Hub.

- Program Owners Buy-in: Current programs supported by SWEF or that will become part of SWEF have different program owner sponsors (e.g., IWS 1/ 2/8, PMS, etc.). The SWEF-Hub design process must consider the needs of these sponsors.

F. CHAPTER SUMMARY

Chapter II showcased the systems engineering process of mission analysis. The team performed a set of SE activities tailored from the INCOSE mission analysis activity section to begin the SWEF-Hub project.

Conversations with the project visionaries led to the identification of the project stakeholders, as well as the formation and refinement of the problem and vision statements for the SWEF-Hub project. The current status and capabilities incorporated into the existing version of SWEF were identified, organized, prioritized, and rated against the vision for the future SWEF-Hub, allowing for the development of a CONOPS for the existing SWEF.

In concert with the project visionaries and with consideration of the project time limitations, the team constrained the scope of the SWEF-Hub project into an outline suitable for a capstone project. Project assumptions and inherent or concrete project constraints were defined.

THIS PAGE INTENTIONALLY LEFT BLANK

III. STAKEHOLDER NEEDS AND REQUIREMENTS DEFINITION

Stakeholder needs and requirements definition is an SE process that takes the raw need statements from the stakeholders' perspective, then refines them into formal stakeholder requirements. During this process, the SWEF-Hub team elicits the stakeholder needs from the participating identified stakeholders, then examines the raw statements from the perspective of the basic mission analysis, while considering the OpsCon developed during the definition process. The team works to refine and distill the requirements to the point where the fundamental stakeholder requirements emerge. Further analysis allows for prioritization of the stakeholder requirements. In accordance with the INCOSE handbook, the formal stakeholder requirements "provide the capabilities needed by users and other stakeholders in a defined environment" (INCOSE 2015, 52).

Figure 12 depicts the SE process of Stakeholder Needs and Requirements Definition. As indicated, during this process the team develops the OpsCon and considers other Life Cycle Concepts. "An OpsCon describes how the system works from the operators' perspective" (INCOSE 2015, 49). An OpsCon delves into the operational environment. It is a lower level view of the system. The OpsCon development step includes identification of the expected set of operational scenarios and the capabilities required for the SWEF-Hub.

Figure 12. Stakeholder Needs and Requirements Definition Process

From the stakeholder requirements and OpsCon considerations flow the identification of the functional requirements and the development of a functional hierarchy. Achievable measures of effectiveness are established. The team sets up processes that ensure traceability all the way from the identified stakeholder needs down to the functional architecture elements. This effort leads to the system requirements definition process.

Figure 13 shows the inputs used in the stakeholder needs and requirements definition process, the process activities, and the outputs that result from the process.

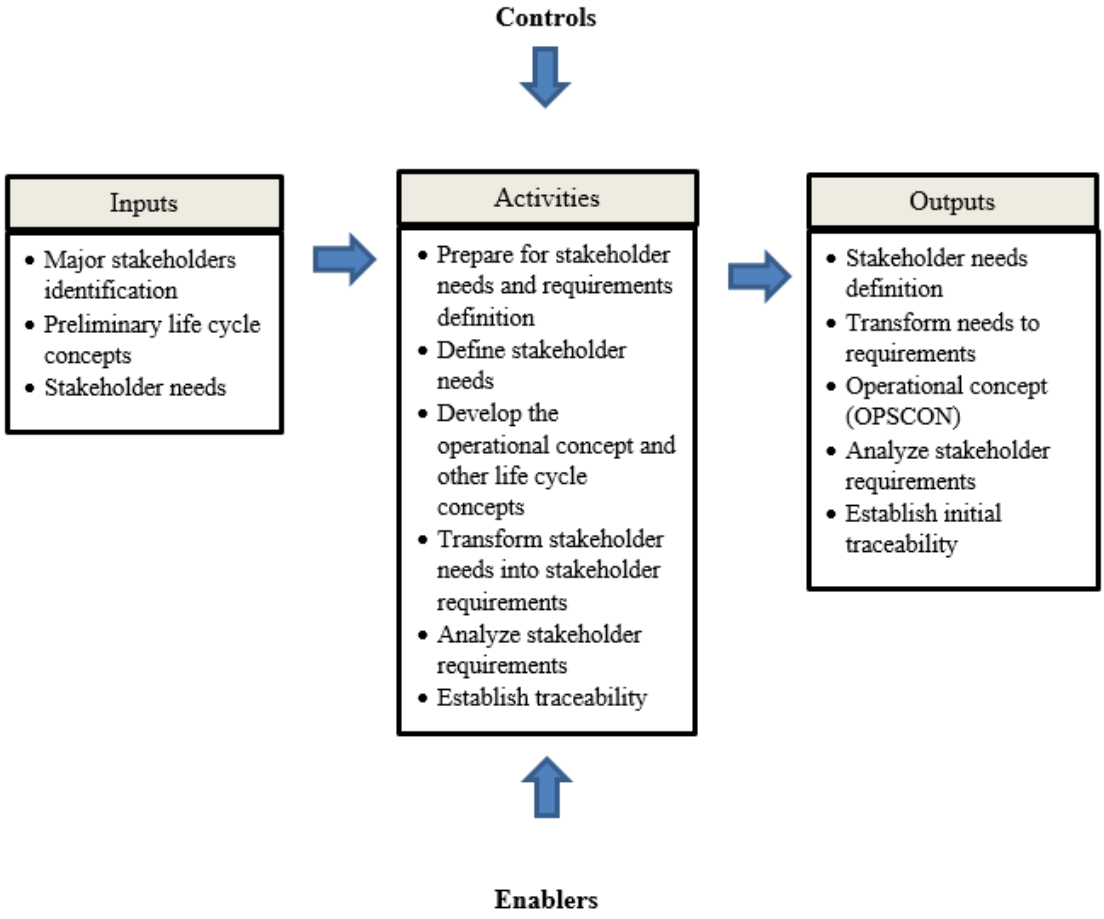


Figure 13. Stakeholder Needs and Requirements Definition Input-Activity-Output Diagram. Adapted from INCOSE (2015).

A. STAKEHOLDER NEEDS DEFINITION

A critical step in the systems engineering process is to define stakeholders' requirements for analysis. The SWEF-Hub team identifies the primitive needs of the stakeholders, then analyzes and transforms them into formal stakeholder requirements. This process includes identifying key individuals, groups, and/or agencies that potentially have a vested interest in the project. The first step leading to stakeholder identification for the SWEF-Hub team involved discussing the project with initial project visionaries and analyzing the original problem statement. The results of these activities included identification of local and remote personnel, commands, key locations, and end users. All of these entities are stakeholders. Through further analysis, the team identified six

stakeholders as primary stakeholders; the prioritization of stakeholder requirements evolves from this ranking. Table 3 depicts the stakeholders and their descriptions.

Table 3. SWEF-Hub Stakeholders and Descriptions

	Stakeholder	**Description**	
1	NSWC PHD	Overall Command where facility will be located	Primary
2	PHD Code 203	NSWC PHD Lead System Engineer	Primary
3	A Department Manager	Air Dominance Department	Primary
4	L Department Manager	Littoral and Strike Warfare Department	Primary
5	S Department Manager	Ship Defense and Expeditionary Warfare Department	Primary
6	PHD Code 206	PHD Distance Support Customer Advocate	Primary
7	Fleet Ships/Aegis Ashore Facilities	Direct Customer of SWEF-Hub Capabilities	Secondary
8	Regional Maintenance Center (RMC)	Support Activity Benefiting from SWEF-Hub	Secondary
9	Surface Force Type Commander (CNSF)	Commander of Fleet Ships	Secondary
10	Naval Sea Systems Command (NAVSEA)	Command for Engineering, building, and supporting the fleet	Secondary
11	Program Executive Office (PEO)	Develops, delivers, and sustains operationally dominant combat systems	Secondary

The basis for narrowing the primary stakeholders down to six is the direct impact of NSWC PHD on one of the primary customers, i.e., the USN fleet; NSWC PHD receives direct work/tasking to support and maintain fleet systems. The impact of the SWEF-Hub project on the primary stakeholders is significant; the enhanced capabilities provided by the SWEF-Hub benefit both their current and future programs.

1. Development of Primitive Needs

The SWEF-Hub team conducted interviews with the primary stakeholders in order to establish the majority of the primitive needs as the stakeholders envisioned them. These interviews included briefing each stakeholder on the project and recording their insights regarding their respective needs and areas of influence. The team examined the current SWEF and its associated entities to establish which needs the current system was supporting. The team arranged tours and question/answer sessions with various distance support entities to help establish the technologies and methodologies currently in use for the SWEF.

Understanding the current needs for the SWEF laboratories is important for the development of the stakeholder needs and requirements for the SWEF-Hub. These existing needs must be supported during the development of the SWEF-Hub and after its implementation. The other important aspect to consider is the additional capabilities that the SWEF-Hub enables for the existing or future labs.

One of the significant primitive needs implied by several of the primary stakeholders involves aspects of the level of interconnection among the laboratories and the combat systems they support in the fleet. Out of more than a dozen individual laboratories within SWEF, only a small fraction of them are significantly interconnected with the systems they support. The majority of the laboratories rely on information provided through existing technology (i.e., email and other electronic media) to replicate or troubleshoot an issue. In some cases, there is no external connection outside the laboratory itself and information must be hand carried into the laboratory space by approved personnel (i.e., couriers). There is delay associated with receipt and transfer of the data, with significant delays associated with the transfer and analysis of classified data. There are additional delays in getting feedback to the customer due to the use of these existing paths and technologies.

Another important implied primitive need involves following NSWC PHD's strategic plan objectives. Current and future sponsors (i.e., program offices) expect the associated laboratories that they fund for NSWC PHD programs to use information from

the fleet elements for their support functions. The laboratories must be able to access the fleet data and use it to recreate reported issues and verify procedures. The laboratories must provide distance support with information resulting from laboratory testing/investigations, with the goal of reducing the overall response time when issues occur. This level of readiness and support to the fleet and external stakeholders aligns with NSWC PHD's strategic plan and its objectives. In a NSWC PHD all hands brief presented on May 31, 2018, the command listed five strategic objectives necessary to improve the fleet support capabilities provided by PHD. The five strategic objectives are:

1. Strategic Objective 1.0
    - Improve integrated combat system readiness
2. Strategic Objective 2.0
    - Accelerate deployment of new capabilities to the fleet
3. Strategic Objective 3.0
    - Improve affordability of integrated combat systems
4. Strategic Objective 4.0
    - Build and shape a mission-focused workforce
5. Strategic Objective 5.0
    - Establish effective cyber ISEA capability/capacity across the integrated combat system life cycle

2. The High-Level Results

Needs were identified by a combination of understanding the current SWEF laboratory capabilities and limitations, incorporating the command strategic objectives, and interviewing the project visionary and primary stakeholders. The needs of each respective area within NSWC PHD were clarified through the use of questionnaires and follow-up interviews of the stakeholders. There are common needs (e.g., fleet support) as

well as unique needs (e.g., shipboard equivalent systems) within each of the main areas of the command that have a stake in SWEF-Hub.

The overall results of the stakeholder needs development process indicate a common theme for requiring a technologically advanced infrastructure for supporting fielded systems in a timely manner, with room for future growth. Developing an architecture that will fulfill these high-level needs requires an understanding of the current capabilities, intermediate efforts, and long-term project goals.

B. TRANSFORMING NEEDS TO REQUIREMENTS

To transform primitive stakeholder needs into stakeholder requirements, the team analyzed and decomposed each stakeholder need into multiple effective needs. Table 4 contains a sample of this transformation from Table 34 in Appendix A. The team used a questionnaire in order to gather enough information to fully understand the individual stakeholder needs. This additional information assisted the team in transforming the stakeholder needs into stakeholder requirements. The result is a list of requirements from each stakeholder that the team prioritized based upon what can be executed in the short term versus long-term goals. Some of the requirements are common to multiple stakeholders based on their needs. In addition to common requirements, there are also common constraints that need to be considered. These include:

1. Physical location of SWEF-Hub
2. Funding upgrades to SWEF-Hub
3. Funding personnel to maintain SWEF-Hub when is not part of a direct program

Table 4. Traceability Table: Stakeholder Primitive Needs to Effective Needs (sample)

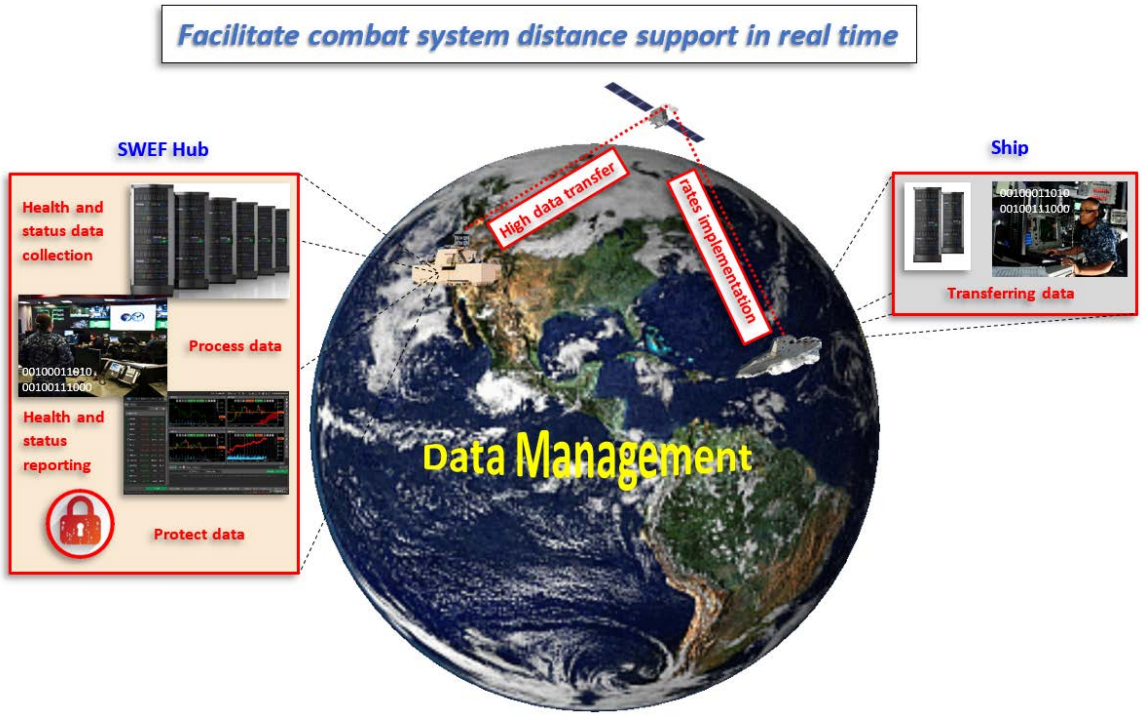
St ID	Stakeholder	Description	PN ID	Primitive Needs (PN)	EN ID. Effective Needs (EN)
St-1	PHD Code 203	NSWC PHD Lead System Engineer	PN-2	Common solution that will provide technical capability across multple systems across the command	7. Common processes across the combat system programs. 8. Technical collaboration of solutions and best practices.
6 Sts			6 PNs		20 ENs

C. OPERATIONAL CONCEPT

The OV-1 diagrams displayed in this section and the associated descriptions capture important operational concepts for the SWEF-Hub. Each OV-1 represents a set of actions that the SWEF-Hub will perform in order to facilitate combat system distance support. An OpsCon is "the first step used to identify, clarify, and document the stakeholders' conceptual operation of the system across the different stages of use and the environments it is to be used in" (INCOSE 2015, 30). It describes what the system will do, and why it will do it, but does not describe how it will do it. An OpsCon is a business level representation for the stakeholder and business needs, rather than a simplified depiction of the system of interest (SOI) developed as a ConOps for the enterprise level of an organization's leadership (INCOSE 2015).

1. Data Management

A representation of data management, consisting of the five elements described below, is shown in Figure 14:



Images from: Buy Mars (n.d.); Telkom Indonesia (n.d.); Turbosquid (n.d.); Wikimedia Commons (2015); Souvannason (2014); Hatzakis (2019); GDPR Informer (2017).

Figure 14. OV-1 for Data Management

a. Health and Status Data Collection

Health and status data coming from combat systems is collected either in real time or from data storage units located on the ship.

b. Data Analysis and Interpretation

Analysis and interpretation of data collected from the ship, accomplished through advanced predictive, retrospective, and other forms of data analysis techniques such as ML, determines the health and status condition of the shipboard combat systems.

c. Health and Status Reporting

Combat system health and status reports, transferred through the SWEF-Hub, inform leadership and lead to actionable decisions.

d. Data Protection Implementation

Cyber security measures, implemented continuously, protect data and information during receipt, transfer, or handling.

e. High Data Transfer Rates Implementation

High data transfer rates reduce the time it takes to transfer data from the ship to the SWEF-Hub and vice versa. High data transfer rates are a factor in reducing the possibility of data or information being stolen during the transfer.

2. Collaboration with the Fleet and Secondary Locations

A representation of SWEF-Hub collaboration with the fleet and secondary locations through real-time distance support, consisting of the five elements described below, is shown in Figure 15:

Images from: Buy Mars (n.d.); Telkom Indonesia (n.d.); Turbosquid (n.d.); Wikipedia (n.d.); Wikimedia Commons (2015); Souvannason (2014); Navy News Service (2015); DHgate.com (n.d.); Amazon (n.d.); RAM Electronics (n.d.).

Figure 15. OV-1 for Collaboration with the Fleet and Secondary Locations

a. Technical and Specialized Support and Recommendations Provision

Data and information are transmitted in both directions, from the SWEF-Hub or secondary locations through the SWEF-Hub to the ship and from the ship back to the SWEF-Hub when resolving an issue.

b. Advanced Situational Awareness Provision

At the SWEF-Hub, real-time data from combat systems or shipboard storage units is collected and processed. The ships' leadership, receiving advanced situational awareness information garnered from the analysis, gains awareness of the ships' combat system present and potential future condition.

c. Preventive and Corrective Action Recommendations Provision

Information transmits in both directions, from the SWEF-Hub to the ship and vice versa, during the process of recommending preventive and corrective actions.

d. Advanced Logistics Support Provision

If a component is nearing failure based on the results of the data analysis, the SWEF-Hub personnel communicates with the ship to inform them of the predicted failure situation and what may happen if the component is not replaced. If necessary, logistics actions begin.

e. Chat, Audio, or Video Communication Provision

Chat, audio or video two-way communications take place as part of the real-time collaboration with the shipboard personnel for troubleshooting, part replacement, or for assessing the physical condition of a combat system.

3. Software and Hardware Troubleshooting

A representation of software and hardware troubleshooting, shown in Figure 16, consists of the two elements described below.

Images from: Buy Mars (n.d.); Telkom Indonesia (n.d.); Turbosquid (n.d.); Wikimedia Commons (2015); Souvannason (2014); Navy News Service (2015).

Figure 16. OV-1 for Software and Hardware Troubleshooting

a. Software and Hardware Problems Traceability and Correction

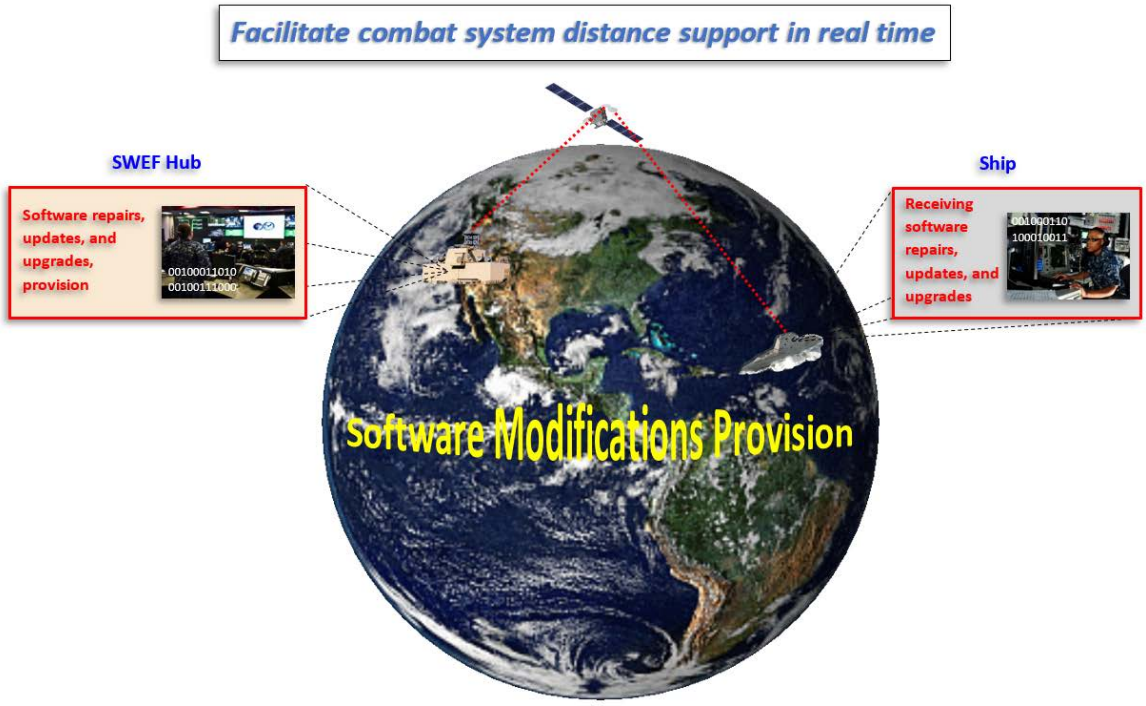
Information transmits in both directions, from the SWEF-Hub or secondary locations through the SWEF-Hub to the ship and vice versa, when resolving an issue.

b. Cyber security Vulnerabilities Detection and Correction

The SWEF-Hub stablishes communication with shipboard personnel in order to troubleshoot a combat system to detect and correct security vulnerabilities.

4. Software Modifications Provision

A representation of the software modifications provision, shown in Figure 17, consists of the three actions described below.



Images from: Buy Mars (n.d.); Telkom Indonesia (n.d.); Turbosquid (n.d.); Wikimedia Commons (2015); Souvannason (2014).

Figure 17. OV-1 for Software Modifications

a. Software Repairs Provision

The SWEF-Hub provides software repairs to the shipboard combat systems when required to fix software problems.

b. Software Updates Provision

The SWEF-Hub provides software updates to the shipboard combat systems periodically in order to keep the combat systems up to date.

c. Software Upgrades Provision

The SWEF-Hub provides software upgrades are provided to the shipboard combat systems when required in order to improve capabilities or replace problematic software.

D. ANALYZE STAKEHOLDER REQUIREMENTS

After identifying the stakeholders' raw needs and transforming them into effective needs, the next step in the stakeholder needs and requirements definition process is to perform a stakeholders' requirements analysis. The purpose of this analysis is to define which operational, functional, physical, and performance requirements are necessary in order to satisfy all stakeholders. The team considers the operational concept, external systems diagrams, and a hierarchy of the objectives in order to perform a stakeholders' requirements analysis. Additionally, the team considered recommendations that four categories or perspectives should be included during the analysis, consisting of system inputs and outputs, system-wide and technology considerations, trade-off considerations, and qualifications (Buede 2016).

The main purpose of this project is to facilitate shipboard combat systems distance support in real time through the medium of the SWEF-Hub and located in NSWC PHD.

(1) The operational requirements identified in the objectives hierarchy are as follows:

1.0 Manage data

2.0 Collaborate with the fleet and secondary locations

3.0 Troubleshoot software and hardware

4.0 Provide software modifications

(2) These operational requirements were expanded into functional requirements as shown below:

1.0 Manage data

1.1 Collect health and status data

1.2 Process data

1.3 Report health and status

1.4 Protect data

1.5 Implement high data transfer rates

2.0 Collaborate with the fleet and secondary locations

2.1 Provide technical and specialized support and recommendations

2.2 Provide advanced situational awareness

2.3 Provide preventive or corrective action recommendations

2.4 Provide advanced logistics support

2.5 Provide chat, audio, or video communication

3.0 Troubleshoot software and hardware

3.1 Trace and correct software and hardware problems

3.2 Detect and correct cyber security vulnerabilities

4.0 Provide software modifications

4.1 Provide software repairs

4.2 Provide software updates

4.3 Provide software upgrades

(3) Conversion of Operational, Functional, Physical, and Performance Requirements into Stakeholders' Requirements.

- SWEF-Hub spaces shall meet top secret space requirements.
- SWEF-Hub shall be designed to maximize use of internal locations for common shipboard systems.
- SWEF-Hub shall provide HVAC systems capable of maintaining adequate temperature for laboratory equipment.
- SWEF-Hub shall be able to exchange data/communication between spaces up to top secret in real time.

- SWEF-Hub shall be able to connect to external sites providing and receiving classified information in real time.
- SWEF-Hub shall capture requirements encompassed in overarching PHD Instructions.
- SWEF-Hub shall adhere to established PHD processes.
- SWEF-Hub shall provide technical changes for review to ensure commonality and best practices are being used in existing and in new labs.
- SWEF-Hub shall provide the architecture for integrated Combat Systems and elements at SWEF for current and future systems.
- SWEF-Hub shall provide shipboard equivalent systems.
- SWEF-Hub shall provide the architecture for seamless integration of both simulated and shipboard equivalent systems.
- SWEF-Hub shall be able to insert shipboard data to recreate issues.
- SWEF-Hub shall provide the architecture for integrated Combat Systems, shipboard networks, and elements at SWEF for current and future systems.
- SWEF-Hub shall provide the capability for integration cyber capabilities for both preventative, reporting, and exploiting vulnerabilities.
- SWEF-Hub shall provide the capability for integration of directed energy systems.
- SWEF-Hub shall provide the shipboard equivalent infrastructure to improve distance support.

Table 5, which appears in the next section, and Appendix A display the initial traceability between the stakeholder needs and the stakeholder requirements.

E. ESTABLISH INITIAL TRACEABILITY

Traceability from the initial stakeholder needs to the final system architecture is an artifact required for a successful SE project. A complete traceability table assists in the validation of the system, i.e., Does the system do what it is designed to do from the stakeholders' perspective? Traceability enables easier modifications and changes later in the project or later in the system's life cycle. The traceability required after the stakeholder needs and requirements definition process should begin with the stakeholders and their primitive needs, progress through their effective needs, and end with the deduced list of formal stakeholder requirements (StR) (INCOSE 2015). Table 5 shows a fraction of the full traceability table, including two stakeholders and their requirements. The numbering scheme used allows a coherent system to track the requirements back to the relevant stakeholder. The full table is displayed in Appendix A.

Table 5. Traceability Table: Stakeholder Needs to StR (Sample)

St ID	Stakeholder	Description	PN ID	Primitive Needs (PN)	EN ID. Effective Needs (EN)	StR ID	Stakeholders' Requirements (StR)
St-1	PHD Code 203	NSWC PHD Lead System Engineer	PN-2	Common solution that will provide technical capability across multiple systems across the command	7. Common processes across the combat system programs. 8. Technical collaboration of solutions and best practices.	SyR-19	The SWEF-Hub requirements shall be captured in overarching PHD Instructions.
						SyR-20	The SWEF-Hub personnel shall adhere to established NSWC PHD security processes and regulations for secured compartments.
						SyR-21	The SWEF-Hub personnel shall prepare technical changes for review, in order to ensure commonality and best practices are being used in existing and future labs.
6 Sts			6 PNs		20 Ens	21 StRs	

F. CHAPTER SUMMARY

Chapter III described the stakeholder needs and requirements definition process followed by the SWEF-Hub capstone team. This process followed from the mission analysis process and leads directly into the system requirements definition process. The stakeholders were interviewed, and their primitive needs were elicited. The primitive needs were transformed into effective needs. OpsCons were built and analyzed, along with deduced system functions to determine formal stakeholder requirements. Traceability from the stakeholders through the formal stakeholder requirements was initiated.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. SYSTEM REQUIREMENTS DEFINITION

The system requirements definition SE process uses the previously refined stakeholder requirements and transforms them into system requirements. This process builds upon the mission analysis and stakeholder requirements definition process and steps toward the architecture definition process; parts of this process directly coincide with the architecture definition process (INCOSE 2015).

As illustrated in Figure 18, the systems requirements definition process begins with the definition of the system functions, accounting for design factors, system constraints, critical characteristics, technical risks, and functional boundaries. From this information, the systems requirements are defined. The second step in the system requirements definition process is the system requirements analysis. This step includes ensuring that the requirements are robust, clear, "and adequately reflect the stakeholder intentions" (INCOSE 2015, 59).

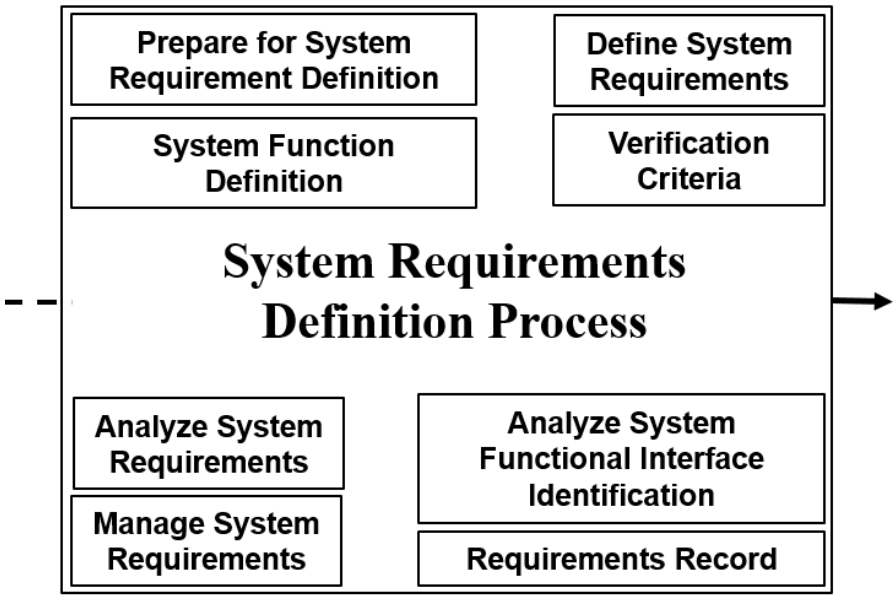


Figure 18. Customized SWEF-Hub SE Systems Requirements Definition Process

Verification criteria are defined in order to specify the critical performance measures that can be used to judge whether the systems' technical goals have been achieved. These verification criteria include MOPs, technical performance measures (TPMs) traceable to the MOEs and measures of suitability (MOSs). The third step in the system requirements definition process is system requirements management. Managing the system requirements includes conferring with the stakeholders to ensure that the system design meets their perceived needs, as well as continuing the traceability from the initial stakeholder requirements onward (INCOSE 2015).

Figure 19 shows the inputs used in the system requirements definition process, the process activities, and the outputs that result from the process.

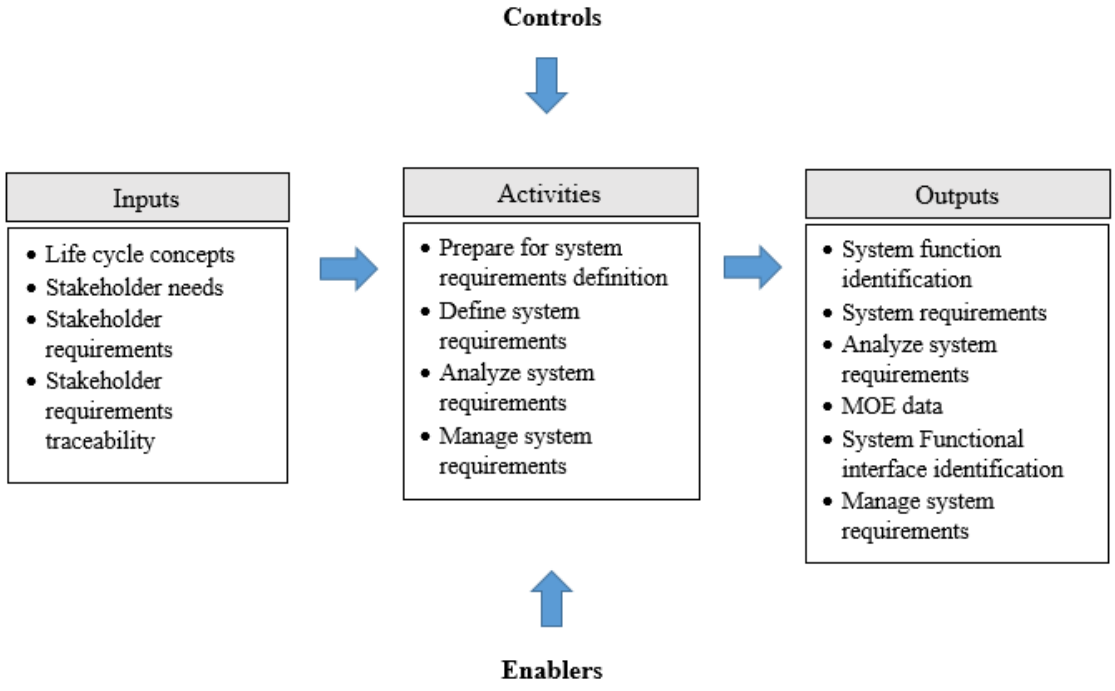


Figure 19. System Requirements Definition Input-Activities-Output Diagram. Adapted from INCOSE (2015).

A. SYSTEM FUNCTION IDENTIFICATION

As part of the system architecture process, it is necessary to develop a functional hierarchy that facilitates the creation of a system architecture. Figure 20 shows the functional hierarchy that illustrates the four first-level elements or pillars of the SWEF-Hub project. Each main element consists of multiple sub-functions as shown.

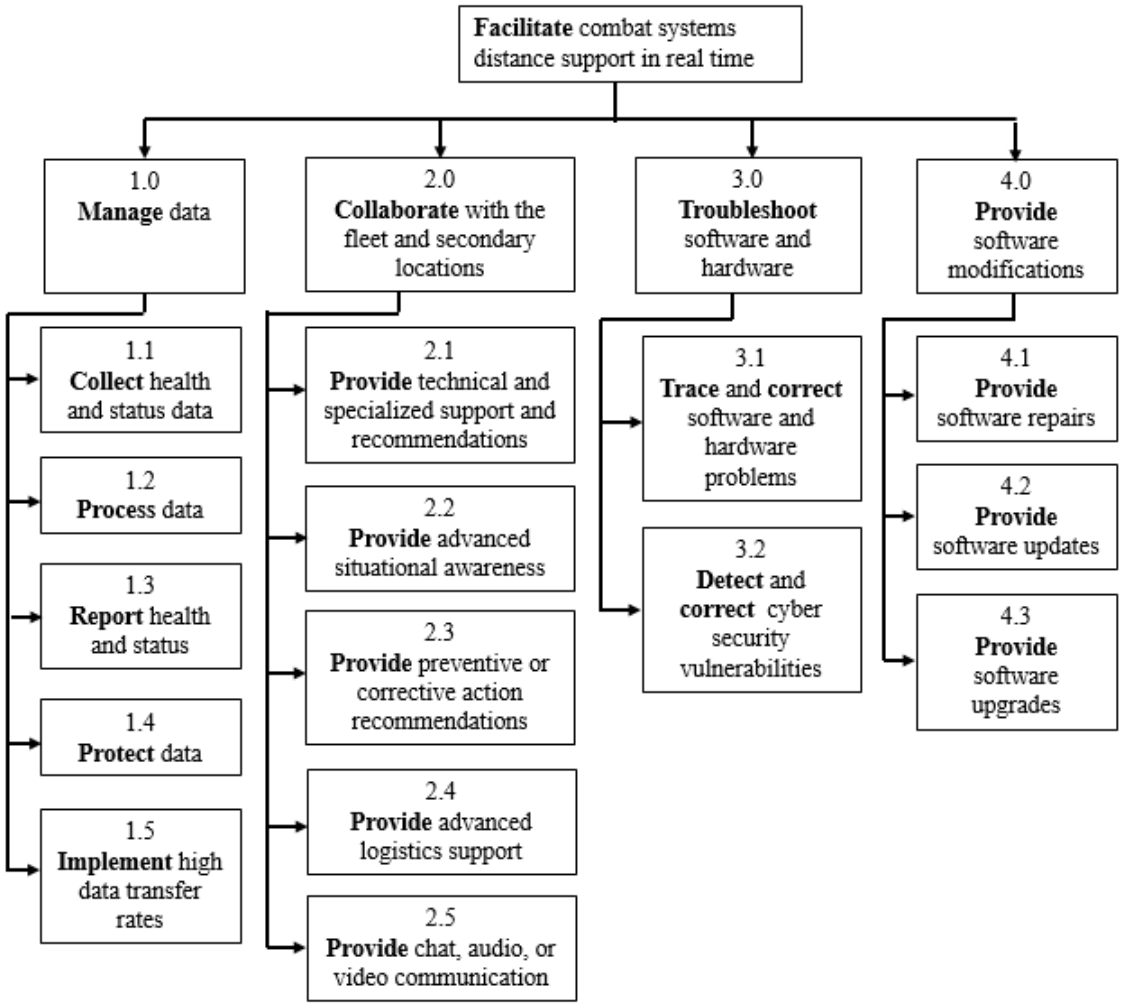


Figure 20. SWEF-Hub Functional Hierarchy Representation

The SWEF-Hub project focuses on the development of a system architecture. The system architecture establishes how to facilitate combat system distance support through

the creation of the SWEF-Hub. The functionality of the four first-level elements is described by the second-level elements.

1. Manage Data

Manage data is the first element on the functional hierarchy. This element involves the collection, analysis, interpretation, reporting, and protection of data. The infrastructure shall be able to receive, process, and store packages of data at high data rates. The following second-level elements are essential parts of data management. Data management must perform the subfunctions: collect health and status data, process data, report health status, protect data, and implement high data transfer rates.

a. Collect Health and Status Data

Real-time health and status data collection is periodically performed, directly or indirectly, on the shipboard systems. Any ship in the fleet with the proper communications infrastructure and combat systems has the capability to transfer data to the SWEF-Hub anytime when normal communications are not restricted. Before data transfers from the ship to the hub, they may undergo a process of data elimination (cleansing), data reduction, and data compression in order to increase the efficiency of data transmission under the restrictions of the available bandwidth.

b. Process Data

After the data is transferred from the ship, analysis and data interpretation occurs using the advanced predictive data analysis (ML) techniques and tools available to the SWEF-Hub; this advanced data processing capability is at the core of the SWEF-Hub functionality. Data decompression occurs upon receipt at the SWEF-Hub to begin the analysis process. During the analysis portion of the process, the data may be enriched, fused, organized, structured, standardized, normalized, classified, integrated, reduced, decomposed, transformed, synthesized, analyzed, etc.; it transforms into meaningful data or information. On occasions when the data analysis processing at the SWEF-Hub is not enough to determine the health and status of a combat system, the data and any information obtained may transfer to a secondary location for additional analysis and final

interpretation. The information that emerges from the analysis process is used to determine the conditions of the combat systems, make predictive decisions, and alleviate upcoming system casualties. Predictive decisions may mean that a replacement part is shipped before a system completely breaks down, or that an SME works to diagnose problems in a system so that it does not break down. Data analysis helps to predict future problems and promotes preventive maintenance.

c. Report Health and Status

The ability to monitor shipboard equipment's health status, view fault alerts and real-time video feed (or representative illustration) of what exactly the sailors are observing and experiencing onboard provides the SWEF-Hub operators a clear picture of problem symptoms; it enables SMEs to provide accurate diagnostics of system problems. The combat system status information resulting from the data analysis may be forwarded to decision-makers, command and control stations, and external supporting organizations. The information is used both to support higher-level decision-making and to provide recommendations to the ship.

d. Protect Data

Data integrity is among the most critical factors for data management. Naval instructions, directives, and guidance are followed to ensure data integrity is maintained. Encryption is used for all data transfers in accordance with cyber security directives. Cyber security implementation at the hub and secondary locations, as a coordinated effort, inhibits the compromising of data while transferring, receiving, and processing occurs. All network hardware involved in the processing of data, as well as personnel who access the data, must operate in accordance with cyber security directives.

e. Implement High Data Transfer Rates

Regarding the process of transferring data between the ship and the SWEF-Hub, high data transfer rates are important. They ensure all relevant data is available for the SMEs and data analysts and promotes accurate and prompt problem resolution. In a hostile environment, transferring data in a short period of time is critical in order to avoid conflicts

with the combat systems computing resources that are essential for the protection of the ship. The data transfer rate is also important for the performance of the total data management process and for faster problem resolution.

2. Collaborate with the Fleet and Secondary Locations

Real-time collaboration is one of the main factors in facilitating combat system distance support from the SWEF-Hub. This function refers to providing advanced situational awareness and real-time distance support using audio and video communications systems. It includes providing technical and specialized support and recommendations from or through the SWEF-Hub from secondary locations. It includes providing preventive and corrective action recommendations to shipboard personnel and enabling advanced logistics support. Real-time collaboration supports the subfunctions: provide technical and specialized support and recommendations, provide enhanced situational awareness, provide preventive or corrective action recommendations, provide advanced logistics support, and provide text, audio, or video communications.

a. Provide Technical and Specialized Support and Recommendations

Situations occur where technical or specialized distance support from the hub or from secondary locations are necessary to resolve problems. Different problems require different solutions and different levels of knowledge. After the source of a present or potential future problem is discovered, technical or specialized solution recommendations are passed to the ship for action. If the source of a problem cannot be identified at the hub, data and information is transferred to a secondary location for further analysis and recommendations. After the source of a problem is identified at a secondary location, recommendations will be transferred to the SWEF-Hub and from there to the ship.

b. Provide Advanced Situational Awareness

The purpose of providing advanced situational awareness is to let decision-makers know in advance when a system casualty may happen if the necessary maintenance steps are not enacted. As previously discussed, data analysis and interpretation using predictive

data analysis techniques makes this possible. The more advance notice there is of a problem in a combat system, the more likely that the ship will be able to avoid a system casualty.

c. Provide Preventive or Corrective Action Recommendations

Once the combat system health and status data transfers to the SWEF-Hub, solutions to existing problems or recommendations for preventative maintenance actions are provided to the ship. Preventive and corrective actions help to extend the life of a combat system. It may help to extend the life of a combat system component while replacement components are shipped.

d. Provide Advanced Logistics Support

Advance logistics support is something that helps to reduce the system downtime. If analytics predict that a component will fail, the replacement component may be sent to the ship days or weeks before the predicted failure occurs. Component replacement helps eliminate a predicted combat system failure before it happens.

e. Provide Chat, Audio, or Video Communications

Having chat, audio, and video as well as text and email communications between the SWEF-Hub and a ship helps to resolve problems without sending ISEA personnel to the ship. This may reduce or eliminate delays in resolving a shipboard problem. Real-time audio/video communications are necessary in some cases in order to enable quick resolution of shipboard problems using shipboard maintenance personnel.

3. Troubleshoot Software and Hardware

As part of providing distance support, troubleshooting of software and hardware is occasionally necessary to resolve issues. Troubleshooting helps to trace and correct system problems; cyber security vulnerability testing may be enabled through troubleshooting the systems. Troubleshooting supports the subfunctions: trace and correct software and hardware problems, and detect and correct cyber security vulnerabilities,

a. Trace and Correct Software and Hardware Problems

Regardless of predictive maintenance activity, systems may fail unpredictably. Distance support and troubleshooting enable the location and correction of system problems. Onboard artificial intelligence systems may be available to assist distance support during system troubleshooting.

b. Detect and Correct Cyber Security Vulnerabilities

Computer-based systems are vulnerable to attack at any time. For this reason, these systems are continuously monitored for these ever-changing threats. Troubleshooting combat systems helps to locate weak areas in cyber security that may be improved. No system is perfect, and technologies are constantly changing; periodic troubleshooting helps to eliminate possible cyber security threats.

4. Provide Software Modifications

Most of today's technologies require some form of software to control system actions. Depending on the situation, some software will require updates, upgrades, or repairs during the life cycle of the system. This type of action restores or improves the performance of a system; it may eliminate cyber security vulnerabilities. The ability to modify software in real time supports the subfunctions: provide software repairs, provide software updates, and provide software upgrades.

a. Provide Software Repairs

Software repairs are often needed to make programs integrate properly with new or existing systems and to fix software vulnerabilities that are not part of regular software updates.

b. Provide Software Updates

Software updates are important and necessary for an operating system (OS) of software application to perform better or resolve issues. Without the software updates, a computer program may start malfunctioning or become vulnerable to cyber-attacks. These updates often may be loaded into the computer automatically and remotely.

c. Provide Software Upgrades

A software upgrade often entails a significant change to a software program. Typically, the original software would be replaced by the upgraded version. A software upgrade is normally not a routine action, nor is it based on as short a time interval as software updates; it is necessary on occasion due to obsolescence or improvements.

B. SYSTEM REQUIREMENTS

System requirements are generated in order to completely characterize the stakeholders' requirements, with established traceability all the way back to the stakeholder needs. They describe requirements (functional and non-functional) at the system level that satisfy the stakeholders' needs and requirements. The relationship between StR and SyR is that one StR may have multiple corresponding SyR. The more system requirements that are developed for each stakeholder requirement, the greater fidelity the overall requirement will have. There is less room for interpretation by the system architect if the requirements sufficiently identify what needs to be developed. The system requirements can be grouped together by the corresponding functional or non-functional requirement. These functions have traceability to the overall stakeholder's requirements and to the systems requirements as shown in Figure 21. Effectively, the StR lead to functional requirements. The functional requirements lead to the determination of MOEs that can be used to ensure the system meets the technical requirements of the stakeholders. Each MOE or measurable characteristic is associated to a functional SyR.

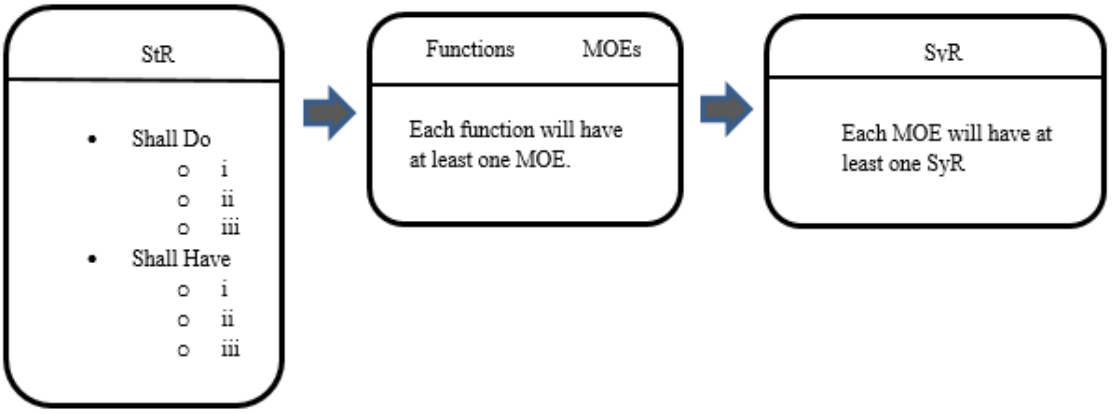


Figure 21. Relationship between StR and SyR

The development of the system requirements involves preparing for the systems requirements definition process by first analyzing the original stakeholder's requirements and identifying any common requirements across the stakeholders. Once the common requirements across the stakeholders are grouped, the systems engineer can proceed with defining the common functions that are being expressed by the stakeholder's requirements (see Table 6 for functions). Specifying the functions and their subcomponents helps to ensure that the definition of the requirements aligns with what the stakeholders require. Once the functions are defined, the process of creating one or more system requirements for each function begins.

The process of creating the system requirements involves multiple tasks. We first must understand constraints that exist within the stakeholders' organization. This helps define requirements that can be accomplished and reduces the amount of work spent on requirements that are not achievable due to constraints and limitations. Additional tasks include understanding technical limitations. This helps to ensure that requirements can be achieved within the time constraints of the project. We must also look at the characteristics of the system being defined. These measures of suitability (MOS) include safety, reliability, security, and supportability (INCOSE 2015). Identifying how these characteristics fit within the functions of the system helps define the overall system requirements. Once the system under development is understood, the process of writing the actual system requirements can begin.

When writing systems requirements, careful consideration must be given to how the requirement is written, not just what the requirement is. In his capstone advisor capacity, Professor Bryan O'Halloran reinforced a requirements-related rule that the appropriate wording must be used (e.g., "shall" or "should") when making a requirements statement. For example, if the requirement must be performed exactly as written, the appropriate word is "shall" when defining the requirement. If there is flexibility in the requirement, the appropriate word is "should." Additionally, the quantity should be considered when developing system requirements. There are functions that should contains multiple system level requirements to ensure that the architecture developed to meet the requirement reflects the overall stakeholders' needs. Too few requirements for functions that are critical to the system from the stakeholders' view might provide too much flexibility and vagueness in how the system is developed. The systems engineer needs to ensure that the critical functions for the project have sufficient system requirements to provide suitable clarity on what is important in defining the solution. SWEF-Hub system requirements have been developed taking into consideration everything mentioned previously. Table 6 provides a snapshot of system level requirements and their overall traceability to the functions and stakeholders' requirements. The stakeholders' requirements are separated into requirements of what the SWEF-Hub shall do (DStR) and characteristics that the SWEF-Hub shall have (HStR). Each StR has identified functional requirements (FR) or non-functional requirements (NFR). Each FR or NFR lead to one or more MOEs and related system requirements (SyR).

Table 6. System Requirements

StR	Stakeholders' Requirements (StR)						
DStR	**Do Stakeholders' Requirements (DStR) (Shall do)**	**FR ID**	**Functional Requirements (FRs)(FRs will lead to functional system requirements)**	**MOE ID**	**Measure of Effectiveness (MOE)**	**FSyR ID**	**System Requirements (FSyR)(these requirements will lead to the physical architecture)(Physical and Software Requirements)**
HStR	**Have Stakeholders' Requirements (HStR) (Shall have)**	**NFR ID**	**Non-Functional Requirements (NFR)**	**NA**	**MOE not needed**	**NFSyR ID**	**Non-System Requirements**
DSyR-0.0	The SWEF-Hub shall be a Navy combat systems distance support center to provide support to the fleet	FR-0.0	The SWEF-Hub shall facilitate combat systems distance support in real time.	MOE-1	Number of requests supported to total requests.	SyR-1	The SWEF-Hub shall have a computer system to install software and process data.
				MOE-2	Number of resolved problems to total problems.	SyR-2	The SWEF-Hub shall have a connection system for texting, audio, and video communications.
				MOE-3	Mean Time To Resolve (MTTRv) a problem.	SyR-3	The SWEF-Hub shall have an AI system to provide distance support.
						SyR-4	The SWEF-Hub shall have personnel (24/7) to provide distance
						SyR-5	The SWEF-Hub shall have combat systems for troubleshooting to recreate scenarios and extract data for analysis.
DSyR-1.0	The SWEF-Hub design shall enable distance support practitioners to securly collect real time combat system health data from deployed ships.	FR-1.1	The SWEF-Hub shall collect health and status data.	MOE-5	Complete vs incomplete data collection.	SyR-0	The SWEF-Hub shall ensure 100% collection of transmitted data.
						SyR-0	The SWEF-Hub should be able to identify gaps in data transmitted 99% of the time.
		FR-1.4	The SWEF-Hub shall implement cyber security.	MOE-9	Ratio of protected attacks to total attacks.	SyR-0	The SWEF-Hub should be able to maintain up to date security definitions and patching.
		FR-1.5	The SWEF-Hub shall implement high data transfer rates.	MOE-10	Data transfer rates. (Consistent data rates)	SyR-0	The SWEF-Hub shall used physical medium capable of high transmission rates.

C. ANALYZE SYSTEM REQUIREMENTS

The system requirements are analyzed to ensure that the statements are complete and clear, and that they meet the stakeholder's perception of what the system is required to do or contain. There must be a viable method available to determine if the system meets the technical demands of the requirements. For that purpose, verification criteria and the associated MOEs are developed. Each MOE will relate to one or more system requirements.

1. System Requirements Verification Criteria

Part of developing good requirements includes ensuring that each requirement is necessary, unambiguous, and verifiable. Developing a solid plan to verify the project's requirements will help answer the question about whether the requirements are verifiable. In order to enable the assessment of technical achievements, critical performance measures have been established. Each system requirement will have an associated MOP or TPM with a defined verification method. The methodologies of analysis used include analysis, demonstration, inspection, and test:

- Analysis (A)—use of analytical data or simulations under defined conditions to show theoretical compliance. "Mainly used where testing to realistic conditions cannot be achieved or is not cost-effective" (INCOSE 2015, 86). Both analysis and simulation may be used when such means establish that the appropriate requirement, specification, or derived requirement is met by the proposed solution (INCOSE 2015).

- Demonstration (D)—a qualitative exhibition of functional performance, usually accomplished with either minimal or no instrumentation. Demonstration (a set of test activities with system stimuli selected by the system developer) may be used to show that system or subsystem response to stimuli is suitable. Demonstration may be appropriate when requirements or specifications appear in statistical terms (INCOSE 2015).

- Inspection (I)—an examination of the item against applicable documentation to confirm compliance with requirements. Inspection is used to verify properties best determined by examination and observation (INCOSE 2015).

- Test (T)—an action by which the operability, supportability, or performance capability of an item is verified when it is "subjected to controlled conditions that are real or simulated" (INCOSE 2015, 86). These verifications often use special test equipment or instrumentation to obtain very accurate quantitative data for analysis (INCOSE 2015).

2. Measures of Effectiveness

The measures of effectiveness are the measures needed to verify to what degree the system meets the mission objectives. The MOEs can be confused with measures of performance (MOPs) because of their similarities (Harney 2011). MOPs refer to measures related to the systems' or subsystems' performance. For example, "Data processed per day" is an MOE, and it provides measures to demonstrate to what extent it reached a predetermined goal, an upper limit for example. On the other hand, "processor speed" is an MOP and it measures how well a system or subsystem can perform. If a system is capable of processing data at levels equivalent or greater than the upper limit in a specific time period, then the system can be considered an effective system. Table 7 lists a total of 20 MOEs that were derived from the functional requirements for the SWEF-Hub. These MOEs will measure the effectiveness of the SWEF-Hub to achieve the main goal of facilitating combat system distance support in real time. If all the requirements are met satisfactorily, then the system is considered completely effective.

Table 7. List of MOEs Derived from Functional Requirements

FRs ID	Functional Requirements (FRs)	MOE ID	MOE Description
FR-0.0	The SWEF-Hub shall facilitate combat systems distance support in real time.	MOE-1	Ratio of supported requests to total requests.
		MOE-2	Ratio of resolved problems to total problems.
FR-1.0	The SWEF-Hub shall manage data.	MOE-3	Data processed per day.
FR-1.1	The SWEF-Hub shall collect health and status data.	MOE-4	Complete vs incomplete data collection.
		MOE-5	Time to gather system data vs file size.
FR-1.2	The SWEF-Hub shall process data.	MOE-6	Data processing rates.
FR-1.3	The SWEF-Hub shall report health and status.	MOE-7	Number of real-time status reports vs number of data packages.
FR-1.4	The SWEF-Hub shall implement cyber security.	MOE-8	Ratio of protected attacks to total attacks.
FR-1.5	The SWEF-Hub shall implement high data transfer rates.	MOE-9	Average data transfer rates.
FR-2.0	The SWEF-Hub shall collaborate with the fleet and secondary locations.	MOE-10	Percentage time the SWEF-Hub was available.
FR-2.1	The SWEF-Hub shall provide technical and specialized support and recommendations.	MOE-11	Number of incidents where technical and specialized support and recommendations were provided by the hub vs the secondary location.
FR-2.2	The SWEF-Hub shall provide advanced situational awareness.	MOE-12	Number of incidents that situational awareness was provided vs the number of complete data packages.
FR-2.3	The SWEF-Hub shall provide preventive or corrective action recommendations.	MOE-13	Number of occasions that preventive and corrective action recommendations were provided vs the number of data packages.
FR-2.4	The SWEF-Hub shall provide advanced logistics support.	MOE-14	Number of parts sent as a result of advanced logistics support vs the number of prevented problems after part replacement.
FR-2.5	The SWEF-Hub shall provide chat, audio, or video communication.	MOE-15	SWEF-Hub can communicate via audio/video – yes/no.

FRs ID	Functional Requirements (FRs)	MOE ID	MOE Description
FR-3.0	The SWEF-Hub shall troubleshoot software and hardware.	MOE-16	Percentage of resolved issues
		MOE-17	Mean corrective maintenance time ($M^{bar}ct$). (Blanchard and Fabrycky 2011, 412)
FR-3.1	The SWEF-Hub shall trace and correct software and hardware problems.	MOE-18	Percentage of corrected software and hardware problems.
FR-3.2	The SWEF-Hub shall detect and correct cyber security vulnerabilities	MOE-19	Percentage of corrected cyber security vulnerabilities.
FR-4.0	The SWEF-Hub shall provide software modifications.	MOE-20	Successful modification – yes/no.

D. SYSTEM FUNCTIONAL INTERFACE IDENTIFICATION

Functional interface identification describes how the different functions will interface. It constitutes another step in the architecture definition process. Functional elements must interact with other elements and that happens through interfaces. In this process, the outputs of one functional element become the inputs of another element. For the purpose of defining and illustrating the different interfaces (how the elements fit with or relate to each other), the N^2 table (or fitting diagram) is one of the tools that can be used. The N^2 table is mainly used for software development, but it can also be used for hardware. As part of the process of eventually identifying the physical elements of the architecture, the N^2 table can help to visualize the relationships between the functional elements of the system. Table 8 does not provide the physical interfaces; however, it provides the interfaces or relationships between the functions. This table facilitated the development of the functional block diagram.

Table 8. N^2 Diagram, Identifying the Interfaces of Functional Elements

Collect health and status data	1.1			x	x									
Process data	x	1.2	x	x	x									
Report health and status		x	1.3	x	x									
Implement cyber security				1.4	x									
Implement high data transfer rates	x	x		x	1.5									
Provide technical and specialized support and recommendations			x	x	x	2.1			x		x		x	x	x
Provide advanced situational awareness			x	x	x		2.2				x				
Provide preventive or corrective action recommendations			x	x	x			2.3			x				
Provide advanced logistics support			x	x	x	x		x	2.4		x				
Provide chat audio or video communication			x	x	x					2.5					
Trace and correct software and hardware problems		x		x	x	x				x	3.1				
Detect and correct cyber security vulnerabilities		x		x	x	x				x		3.2			
Provide software repairs				x	x	x		x		x	x	x	4.1		
Provide software updates				x	x	x		x		x	x	x		4.2	
Provide software upgrades				x	x	x		x		x	x	x			4.3

E. MANAGE SYSTEM REQUIREMENTS

As part of managing system requirements, the team ensured the project's major stakeholders remained engaged and informed of the decisions made during requirements development. Regular reviews of the system engineering process for the SWEF-Hub, referred to as an In-Progress Review (IPR), facilitate the stakeholder engagement. This conversation began with the first IPR, then continued through questionnaires, email communications, and additional IPRs through project completion. The goal is to ensure that the requirements adequately reflect the intentions of key stakeholders. Feedback obtained to date from major stakeholders has been incorporated in a traceable manner. The approach towards traceability includes a requirements verification traceability matrix (RVTM) housed in a Microsoft Excel worksheet that includes every stakeholder's needs, function allocations, system requirements, and their respective critical measures of performance. These measures include MOPs, MOEs and verification information. Additional information, collected in order to clearly define interfaces and to ensure architecture elements, are identified and documented. Documenting every one of these elements provides a baseline for configuration management.

After transforming the stakeholders' needs into requirements, the requirements are placed into a RVTM. Refer to Table 9. This allows traceability once the system requirements are formed.

The system requirements are developed by refining the stakeholders' needs and requirements, creating a system architecture for the design of the SWEF-HUB. Functional requirements are developed to assist in creating system requirements that satisfy the stakeholders' requirements.

Table 9. Traceability from StR to FRs (MOEs) and SyR (MOPs)

StR ID	Stakeholders Requirements (StR)	FR ID / NFR ID	Functional Requirements (FRs) / Non-Functional Requirements (NFR)	MOE ID	Measure Of Effectiveness (MOE)	SyR ID / NSyR ID	System Requirements (SyR) / Non-System Requirements (NSyR) (Non-functionally related)	MOP ID	Measures Of Performance (MOP)
SyR-1	The SWEF-Hub design shall enable distance support practitioners to securely collect real time combat system health data from deployed ships.	FR-1.1	The SWEF-Hub shall collect health and status data.	MOE-4	Complete vs incomplete data collection.	SyR-44	The SWEF-Hub shall ensure succesful collection of transmitted data is near 100%.	MOP-14	Percentage of data collected.
						SyR-5	The SWEF-Hub shall identify gaps in data transmitted 99% of the time.	MOP-3	Percentage Gap identification.
21 StRs		20 FRs		20 MOEs		46 SyRs		14 MOPs	
		12 NFRs				8 NSyRs			

Next, the measures of performance (MOPs) are developed along with the requirements to satisfy the MOPs. A MOP is "the 'implementation' measure of success that should be traceable to the MOEs and MOSs with the relationships defined" in the RVTM and requirements database (INCOSE 2015, 59). The MOPs are the measures needed to verify to what degree a system capable of performing or achieving pre-specified technical objectives (Harney 2011). For example, "processor's speed" is a MOP, and it will define how well a processor can perform. If the processor's speed is low, the processor will be inadequate for the next higher assembly; if the processor is capable of high speeds, the next higher assembly will have no problems performing its related tasks. Table 10 lists a total of fourteen MOPs that were derived from applicable system requirements; i.e., requirements that are related to functionalities. These MOPs will measure the performance of the system of interest, the SWEF-Hub. If all the parts perform satisfactorily, the performance of the entire system will also be satisfactory (INCOSE 2015).

Table 10. List of MOPs Derived from System Requirements

SyR ID	**System Requirements (SyR)**	**MOP ID**	**Measures Of Performance (MOP)**
SyR-1	The SWEF-Hub shall provide reports on detected attacks in real time to system owners.	MOP-1	Number of status reports per number of data packages per day.
SyR-3	The SWEF-Hub shall be able to provide status and summarized reports on data being transmitted as well as data received/archived to system owners.		
SyR-4	The SWEF-Hub shall be capable of processing data by validating, sorting, summarizing, and aggregation in real time.	MOP-2	Processor's speed.
SyR-2	The SWEF-Hub shall analyze data received for degraded performance to detect failure trends in order to provide automatic reports to system owners when patterns are detected.		
SyR-20	SWEF-Hub shall have a high-speed processor able to process at a minimum two sets of shipboard data at a given time.		
SyR-5	The SWEF-Hub shall identify gaps in data transmitted.	MOP-3	Percentage Gap identification.
SyR-7	The SWEF-Hub shall provide automatic recommendations to system owners when	MOP-4	Recommendations per issue per day.

SyR ID	System Requirements (SyR)	MOP ID	Measures Of Performance (MOP)
	systems are under test and after issues are identified.		
SyR-9	The SWEF-Hub shall use a physical medium capable of high transmission rates.	MOP-5	Data transfer rate.
SyR-43	The SWEF-Hub shall have a communication system capable of supporting high speed communications of rates.		
SyR-10	The Spaces within SWEF-Hub facilities shall include entry/exit physical security systems and measures for up to top secret level in accordance with security regulations as applicable.	MOP-6	Number of intrusions per days.
SyR-16	The SWEF-Hub shall have an open system capable of being upgraded with minimal impact or down time no greater than 48 hours.	MOP-7	Upgrade downtime.
SyR-17	The SWEF-Hub shall be capable of software installations of shipboard systems within one-hour period.	MOP-8	Software installation speed.
SyR-19	The SWEF-Hub shall load external shipboard data into its shipboard systems within eight hours.	MOP-9	Data load-rate.
SyR-25	The SWEF-Hub shall load external shipboard data for analysis within eight hours.		
SyR-26	The SWEF-Hub shall be able to load at a minimum two sets of external data for analysis.		
SyR-29	The SWEF-Hub shall have a cyber security system to provide continuous internal and external cyber defense capabilities.	MOP-10	Protected attacks per total attacks per day.
SyR-39	The SWEF-Hub shall use fiber optics and ethernet cable infrastructure for high speed communications.	MOP-11	Frequency capacity.
SyR-31	The SWEF-Hub shall use fiber optics and ethernet cable infrastructure to provide secured internet connectivity.		
SyR-32	The SWEF-Hub shall have an alert system to provide automated alerts when potential cyber threats are detected to internal SWEF-Hub managers and approved NSWC PHD personnel.	MOP-12	Ratio of identified/processed to reported threats.
SyR-33	The SWEF-Hub shall contain an air conditioning system to maintain the space ventilated between 50–75 degrees Fahrenheit.	MOP-13	Heat removal rate.
SyR-44	The SWEF-Hub shall ensure 100% collection of transmitted data.	MOP-14	Percentage of data collected.

F. CHAPTER SUMMARY

Chapter IV described the system requirements definition SE process. System functions were allocated to the stakeholders' requirements. The functions were translated into system requirements and assigned MOEs. Traceability was continued from the stakeholders' requirements all the way through the system requirements. The system requirements definition process leads next to the system architecture process.

V. ARCHITECTURE DEFINITION PROCESS

The SWEF-Hub team follows the general plan for architecture definition as outlined in the INCOSE handbook. The general plan outlined in the handbook allows the user to follow a structured format that contains important points that need to be considered to define the SWEF-Hub architecture. The SWEF-Hub team provides two architectures for the SWEF-Hub, a near-term architecture and a long-term architecture. This chapter provides the process the team used to develop the two architectures for the SWEF-Hub, then presents the artifacts of the two architectures in separate sections. Figure 22 represents the customized SE architecture definition process used by the SWEF-Hub capstone team.

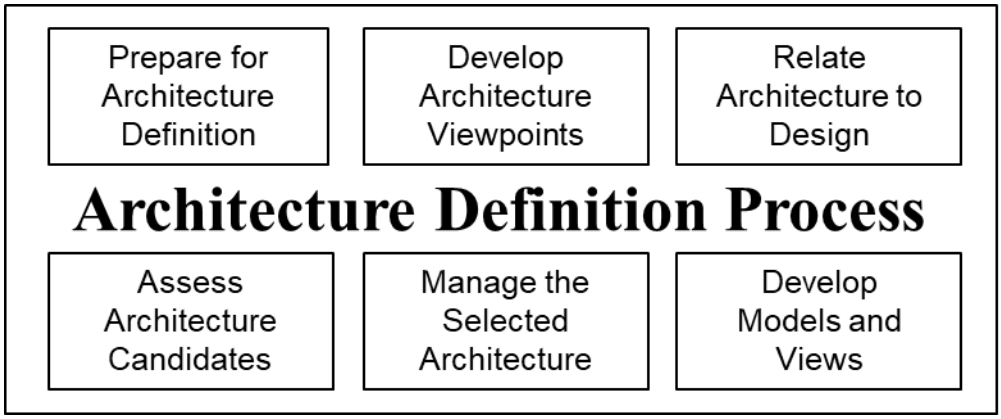


Figure 22. Customized SWEF-Hub SE Architecture Definition Process

Each of these steps has multiple subtasks that must be accomplished in order to generate a valid and useable architecture definition.

As stated in ISO/IEC/IEEE 15288, “the purpose of the architecture definition process is to generate system architecture alternatives, to select one or more alternative(s) that frame stakeholder concerns and meet system requirements, and to express this in a set of consistent views” (INCOSE 2015, 64). the architecture definition process diagram shown in Figure 22 has six steps. These include preparing for architecture definition, develop architecture viewpoints, relate architecture to design, assess architecture

candidates, manage the selected architecture, and develop models and views. Team SWEF-Hub met with the primary stakeholders in order to develop two architectures, the near-term (less than three years) architecture and long-term (ten years out) architecture. The near-term architecture consists of the immediate architecture that will evolve to become the long-term architecture. The near-term architecture does not have an artificial intelligence system such as ML, but it does have a database that will be used to collect data in order to build a large bank of information. The long-term or future architecture consists of an artificial intelligence system that utilizes different databases and tools to provide long distance support in real time.

Figure 23 shows the inputs used in the mission analysis process, the process activities, and the outputs that result from the process.

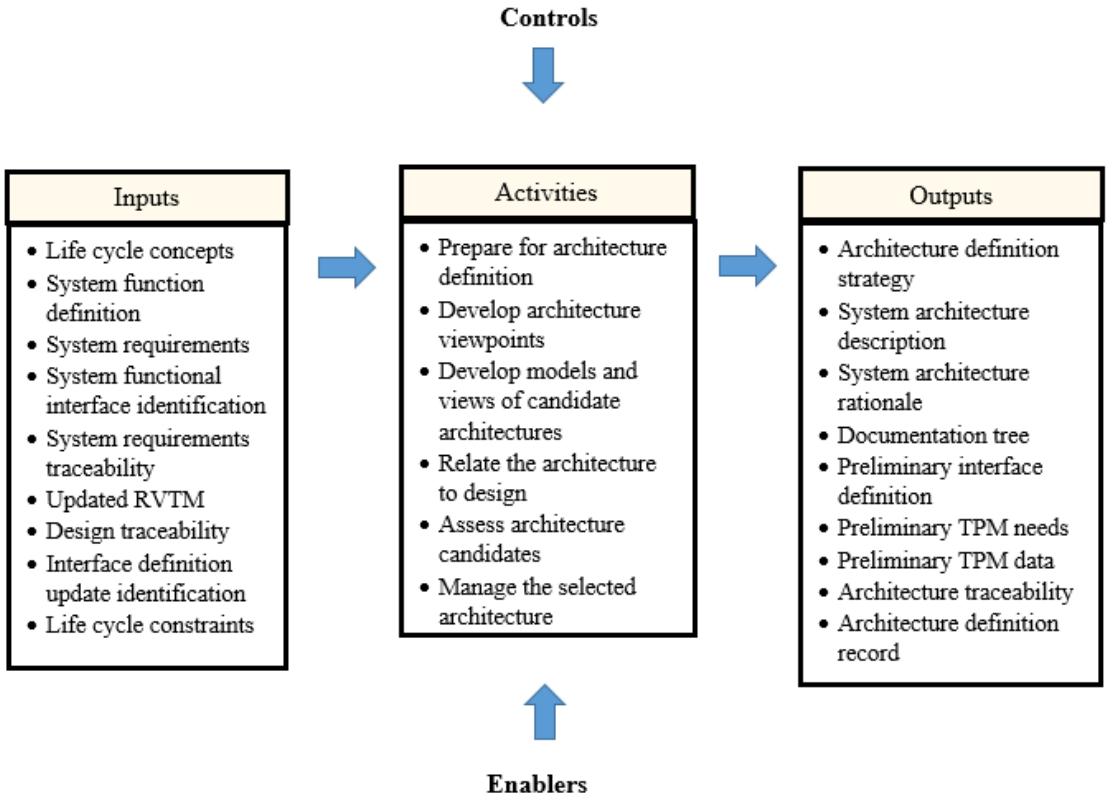


Figure 23. Mission Analysis Input-Activity-Output Diagram. Adapted from INCOSE (2015).

A. PREPARE WHAT IS NECESSARY TO DEFINE THE ARCHITECTURE

Before the architecture is started, it is important to have the inputs ready for use during the process activities. There are three subtasks included in the preparation step as they pertain to the SWEF-Hub project. They are:

- The system requirements are analyzed to determine those that are functionally or non-functionally related to the SWEF-Hub.
- The team determines whether or not the stakeholders intend for the project to proceed beyond one life cycle.
- The team builds a plan and elaborates upon it in order to lead towards the creation of the architecture.

1. System Requirements Analysis

Determination of which system requirements are functionally or non-functionally related to the system facilitates determination of the elements that make up a solution for the architecture. The elements that are included in the architecture cover both the "shall do" and "shall have" parts of the requirements, tracing back to the initial stakeholders' requirements.

2. Stakeholder Intentions for the Project beyond One Life Cycle

Answering the question of whether or not the project is intended to proceed beyond the initial life cycle affects how the architecture is defined. Depending on the project, it might have a contemporary purpose that is expected to be superseded or eliminated over the project's initial life cycle. In the case of the SWEF-Hub, the stakeholders' plans are to extend the life of the SWEF-Hub system by integrating upgrades and/or expanding the coverage of the system to include new combat systems and support system entities. Any potentially improved version of the SWEF-Hub system would necessarily encompass the functions and relevant precepts of the SWEF-Hub system.

3. Building and Elaborating on a Plan That Leads to the Creation of an Architecture

The plan the SWEF-Hub team builds defines the approach for each step of the architecture creation process and states the "roadmap and strategy, as well as the methods, modeling techniques, tools, and the need for enabling systems, products, or services" (INCOSE 2015, 66). The plan explains the evaluation of the architectures to ensure that all requisite requirements are considered and guarantees that the system is obtainable in the near-term (three-year timeframe) and as projected further into the future (ten-year timeframe). Following the six steps outlined in the INCOSE handbook helps to establish a properly developed plan that ensures that the necessary areas and tasks pertaining to an architecture definition are addressed.

B. CREATE THE VIEWPOINTS OF THE ARCHITECTURE

The main subtask included in the viewpoint creation step as it pertains to the SWEF-Hub project is that of developing the various viewpoints. The general sequence of events in developing viewpoints for the SWEF-Hub flows from realizing the stakeholders' concerns, to determining their objectives, leading toward the establishment of viewpoint solutions as pertains to the SWEF-Hub

In order to develop the architecture viewpoints of the SWEF-Hub, it is important to pay attention to the different stakeholders' concerns. Each stakeholder has one or more concerns that they want addressed, some of which overlap between stakeholders. From these individual concerns, the objectives are generated. Effectively, once the SWEF-Hub team determines the objectives of the stakeholders, they generate viewpoints of the SWEF-Hub that are the abstract representations of the SWEF-Hub that stakeholders are visualizing. Similar to the stakeholders' concerns, some of the stakeholders' viewpoints will overlap (ArchiMate n.d.). Architectural views or diagrams of the SWEF-Hub are created in order to illustrate the stakeholders' viewpoints. For example, one viewpoint is the concept of providing services to the fleet. The stakeholders see the SWEF-Hub as a center that will provide different services to the fleet. To illustrate this idea, different views

or functional block diagrams are created. Because the concept of providing services to the fleet is broad, it embodies several viewpoints.

C. CREATE THE VIEWS AND MODELS OF THE ARCHITECTURE

In order to create views and models also known as diagrams, a process with techniques or methods is necessary. The process guides the creation and definition of the views and models of the SWEF-Hub architecture. From the different top-level models and views, the team develops other models or views in order to properly define the architecture. An overview of what is done in this process is:

- Techniques and tools are used in the development of the architectures.
- From the top-level models, other models are developed in order to define the architecture.
- Candidate architecture models are created as part of the architecture development.
- The architecture entities that will be part of the SWEF-Hub to address the highest priority requirements are determined.
- Constraints and risks are determined.
- The models and views are analyzed for consistency in order to determine issues that need to be resolved.
- More system requirements are developed if new elements are created.
- Models and views for the near-term are developed.
- Models and views for the long-term are developed (at the ten years mark).

1. General Process Described

In the following process, techniques or methods are used to derive the architecture diagrams (views) intended to illustrate the architecture of the SWEF-Hub. At the end of these process, three main types of diagrams are defined:

- Functional diagrams
- Physical diagrams
- Interface diagrams.

a. Determine the Objectives

The first step in the process is to determine the objectives. The SWEF-Hub team analyses the stakeholders' concerns and needs in order to determine the stakeholders' true objectives. If a stakeholder is concerned about a current situation, the concern triggers a need, and the need helps to set an objective. For example, a stakeholder(s) concern involves the fact that several of a ship's help requests come from different locations (entities), not directly from the ship itself. This concern triggers a need for a central point where all ships' help requests, related to combat systems, initially go to, a hub. This conceptual hub becomes an objective. Once the SWEF-Hub team determines the objectives, they can present them using an objectives hierarchy diagram or other methods.

The following list includes the stakeholders' objectives derived from the stakeholders' concerns and needs:

- Improve customer service.
- Increase situational awareness.
- Improve combat system's reliability by providing:
    - predictive assessments
    - preventive and corrective maintenance recommendations.
- Provide real-time collaboration.

- Provide immediate response in emergency situations.
- Provide technical and specialized distance support from a focalized point.
- Limit the need of on-site field technicians and engineers.
- Employ advanced technological concepts.

b. Determine the Viewpoints

After determination of the objectives, the team determines or constructs the viewpoints. As stated earlier in the architecture definition process, the viewpoints are the abstract representations of the SWEF-Hub (ArchiMate n.d.).

The following listing includes the viewpoints of the SWEF-Hub architecture taken from the Department of Defense Architecture Framework (DoDAF) to represent how the stakeholders envision the SWEF-Hub:

- The All viewpoint describes the total idea of the SWEF-Hub that relates to all the viewpoints (Dodcio 2010).
- The Capability viewpoint refers to the requirements concerning the capability of the system, timing of the system delivery, and capability of the system that will be deployed (Dodcio 2010).
- The Data and Information viewpoint discusses the data relationships and congruency of the architectural structures with regard to the “capability and operational requirements, system engineering processes, and systems and services” (Dodcio 2010, 1).
- The Operational viewpoint covers the actions, operational situations, and requirements concerning the support of capabilities (Dodcio 2010).
- The Services viewpoint refers to the design that provides the solutions concerning to the “performers, activities, services, and their exchanges” to

provide the support for “operational and capability functions” (Dodcio 2010, 1).

- The Standards viewpoint refers to all pertaining laws, policies, standards, guidance documents, predictions, and restrictions relating to the operational and capability requirements, systems, services, and processes pertaining to system requirements (Dodcio 2010).

c. Determine the Top-level Functions

In the next step, the SWEF-Hub team determines the top-level functions of the SWEF-Hub. From the top-level functions, the team determines the next level functions in order to create a functional hierarchy diagram. In order to determine these functions, the team analyses the stakeholders’ viewpoints and requirements to determine the functionalities of the SWEF-Hub. Because the SWEF-Hub is intended to be the focal point for passage of all data, and because most of the SWEF-Hub functions, if not all, involve transporting data, the team focuses on combat systems data and communications during the creation of the functions.

The following listing includes the top-level functions and subfunctions:

- Facilitate combat systems distance support in real time.
    - Manage data.
        - Collect health and status data.
        - Analyze and interpret data.
        - Report health and status.
        - Implement cyber security.
        - Implement high data transfer rates.
    - Collaborate with the fleet and secondary locations.

        - Provide technical and specialized support and recommendations.
        - Provide advanced situational awareness.
        - Provide preventive and corrective action recommendations.
        - Provide advanced logistics support.
        - Provide audio and video communication.
    - Troubleshoot software and hardware.
        - Trace and correct software and hardware problems.
        - Detect and correct cyber security vulnerabilities.
    - Provide software modifications.
        - Provide software repairs.
        - Provide software updates.
        - Provide software upgrades.

After the team establishes these functions, they are used to create the functional requirements that would lead to the creation of some of the system requirements or system functional requirements. Consequently, these requirements lead toward creation of the physical architecture.

d. Consider the Levels of Data Connectivity

After the team determines the top-level and sub-level functions, it considers the top-level and sub-levels of data connectivity. For example, when considering a communications data connection, a determination of whether the communication is a loop or merely a one-way communication path must be made. Normally, combat systems data transfer happens in a one-way path, and the response is communications data transfer (also

in a one-way path). In some situations, the response is a combat systems data transfer in the form of a software repair, software update, or software upgrade.

e. Assign Groups and Hierarchies of Responsibility to Functions

Once the team creates the main top-level and sub-level functions, it determines who will perform all the actions of the functions. The team determines the groups or entities who perform the actions at the SWEF-Hub and those who interact with the SWEF-Hub. The team sets the general sequence of who performs which action and when the action is performed. It is also important to know who in general should be first, second, third, and so forth.

1. Customer (Not part of the SOI).
2. Help desk at SWEF-Hub.
3. Secondary location (Not part of the SOI).

f. Determine the Top-level Actions for Each Group or Individual Entity

After determining the groups and individual entities, the team assigns them the corresponding top-level actions that they will perform.

4. Customer requests help.
5. Help desk directs communication and is the first in line to provide support.
6. Secondary location analyzes problems that were not solved at the SWEF-Hub.

g. Determine the Needs that Trigger Actions and the Results of Those Actions (Similar to Inputs and Outputs)

The second level and, if necessary, the third level and lower level actions for each group or individual are determined. The team simplifies and reduces action names to fit in the blocks. The team determines the interfaces between the different actions and develops an N^2 or other diagram to display the relationships.

h. Action Diagram Creation

The team creates action diagrams. The actions are organized as first, second, third, and so on. The team adds “OR” nodes between actions and IF loops as necessary, they are added. The team performs iterations of this process in order to further define the functional diagrams or views of the functional architecture.

i. Physical Architecture Definition

After development of the action diagrams needed to define the functionalities of the SWEF-Hub, the team defines the physical architecture. In this step, the team determines the elements and sub elements necessary to perform the actions. The team ensures that no system requirement is ignored during this process. Allocation matrices are used for determining whether all requirements have been considered and if more elements are needed.

j. Physical Element Hierarchy Diagram Implementation

The team creates a hierarchy diagram for physical elements through consideration of the functions and action diagrams. The physical element hierarchy diagram leads to the development of an interface diagram. The interface diagram is used to define the links or interfaces between the physical elements. In this diagram, cables, switches, connectors, and other interphases are defined.

k. Implementation of Other Diagrams

If necessary, other diagrams are created to define other portions of the architecture.

2. Tools Used

The tools used for the development of models, views, and allocation matrices are Microsoft Excel and Innoslate. Each tool had a different purpose. For tables and allocation matrices, Excel is considered sufficient. For hierarchy diagrams and block diagrams, Innoslate is considered necessary and sufficient.

3. Models and Views

The following architectural candidate models and views help to define the SWEF-Hub architecture:

- The N^2 diagram shows the interfaces between the functional elements and facilitates the creation of the functional diagrams (see Table 8 in Chapter V Section D).
- The functional models and views show the system functions and illustrates how these functions interact with other functions. They show the different functional process flows.
    - Action flow diagrams created.
        - Combat system health.
        - Condition-Based Maintenance (CBM).
        - Raw data collection.
        - Troubleshoot.
        - Software upgrade.
        - Secondary collaboration.
- The structural model shows the physical elements.
    - Physical architecture diagrams.
    - Function to physical mapping.
- The physical interface models illustrate the interfaces between the physical elements.
    - The internal and external physical interfaces are defined.
        - Internal interfaces: those within the SWEF-Hub.

- External interfaces: those between the SWEF-Hub and secondary locations.

4. The SWEF-Hub Architecture Is Divided in Two: The Near-Term and Long-Term Architectures

The two architectures have different views that illustrate the overall idea of the SWEF-Hub. The near-term architecture is the simpler of the two because it does not encompass the concept of machine learning. The team uses the near-term architecture as the starting point for the long-term architecture. The long-term is more complex but provides a greater benefit.

D. NEAR-TERM FUNCTIONAL ARCHITECTURE

Near-term architecture defines an architecture that can be implemented within a three-year timeframe. It consists of the initial architecture that will evolve into the long-term architecture.

The following diagrams illustrate the near-term architecture:

1. Combat Systems Health Near-Term Action Diagram Description

The combat systems health near-term action process contains two elements: the ship element and the SWEF-Hub element. The ship element initiates a scheduled combat systems data query, see action (1.2) in Figure 24, then securely sends the data to the SWEF-Hub (1.3). The SWEF-Hub receives (1.4), analyzes (1.5), categorizes (1.6), and stores the repair history data (1.7) in the database. The SWEF-Hub is manned 24/7, the personnel are biometrically authenticated, and its operational status is continuously monitored (1.1).

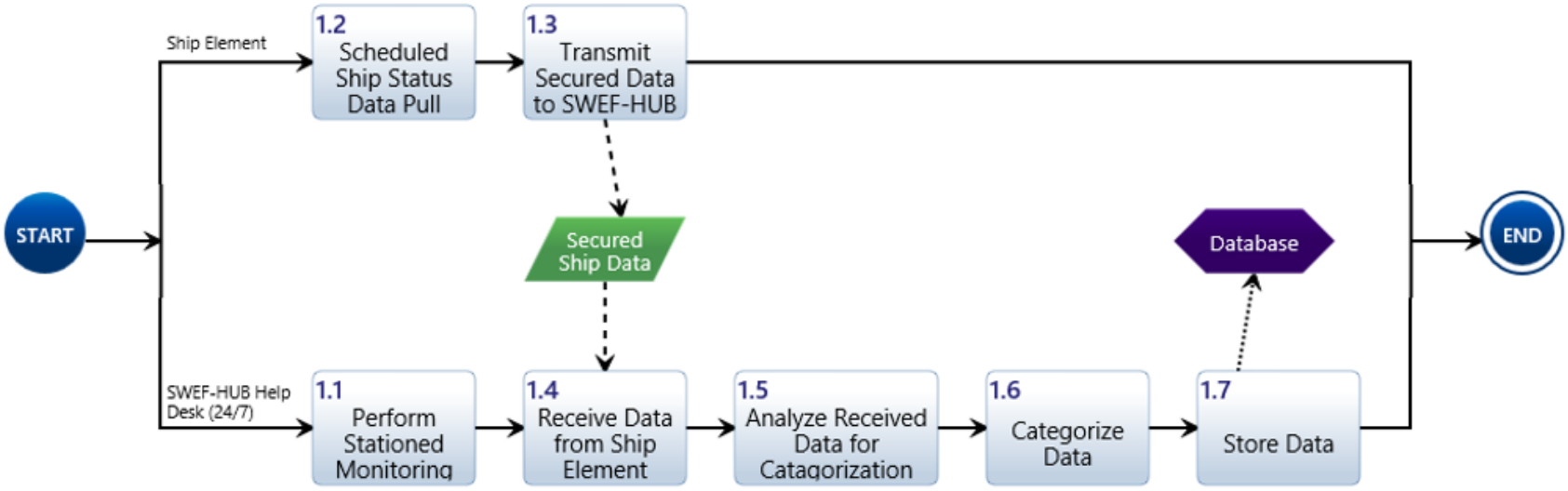


Figure 24. Combat Systems Health Near-Term Action Diagram

2. Condition-Based Maintenance Near-Term Action Diagram Description

Three elements are involved in the CBM process for near-term action: the ship element, the SWEF-Hub help desk, and the technical center personnel. Starting with the ship element, onboard maintenance personnel execute equipment maintenance actions that are automatically scheduled, see action (2.1) in Figures 25 and 26. Figure 25 displays the full action diagram for reference, while Figures 26 and 27 show the details of the diagram. Hereafter, actions are identified by number, e.g., (11.1) and functions that are re-used will appear with their original function number. When the ship element completes the action, the notice of completion (NOC) data is securely emailed to the SWEF-Hub help desk (2.2).

The SWEF-Hub is manned 24/7, the personnel are biometrically authenticated, and its operational status is continuously monitored (1.1). After the SWEF-Hub receives the NOC data (2.3), the appropriate technical center is identified (2.4), and the SWEF-Hub transmits the NOC to the technical center (2.5). Subject matter experts within the technical center receive (2.6) and analyze the data (2.7). Once the technical center determines a potential solution, it sends the proposed course of action (COA) to the SWEF-Hub (2.8). The SWEF-Hub receives the COA from the technical center (2.9), identifies the ship element (2.10) and transmits the COA to the ship element (2.11). The ship element receives (2.12) and implements (2.13) the recommended COA. Upon completion (2.14), the ship element generates and sends a relevant NOC to the SWEF-Hub (2.15). The SWEF-Hub receives the data (2.16), then passes the NOC (2.17) to the technical center. The technical center receives it (2.18), closes it (2.19), and then sends a final closeout message to the SWEF-Hub (2.20). The SWEF-Hub receives the closeout issue message (2.21) and stores the repair history data (1.7) in the database.

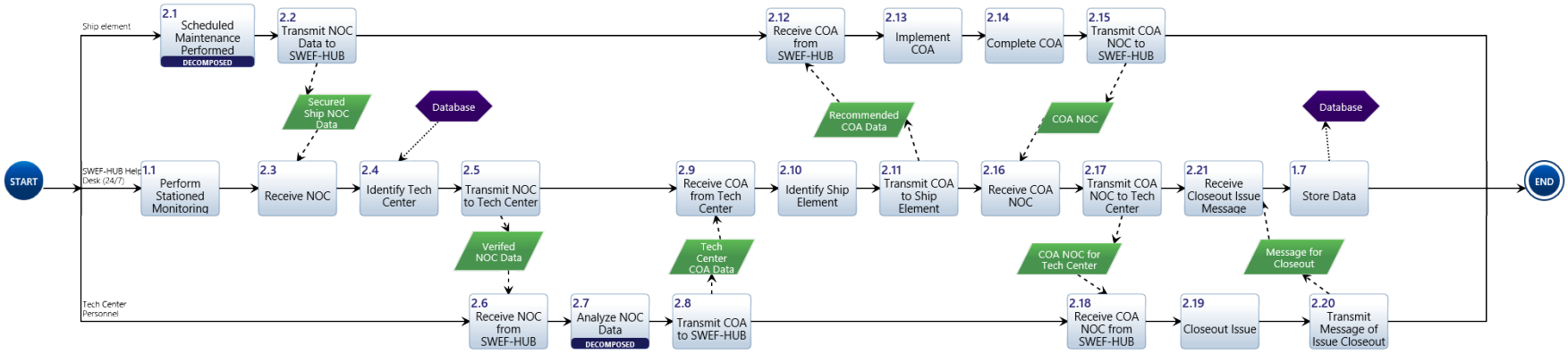


Figure 25. Condition-Based Maintenance Near-Term Action Diagram

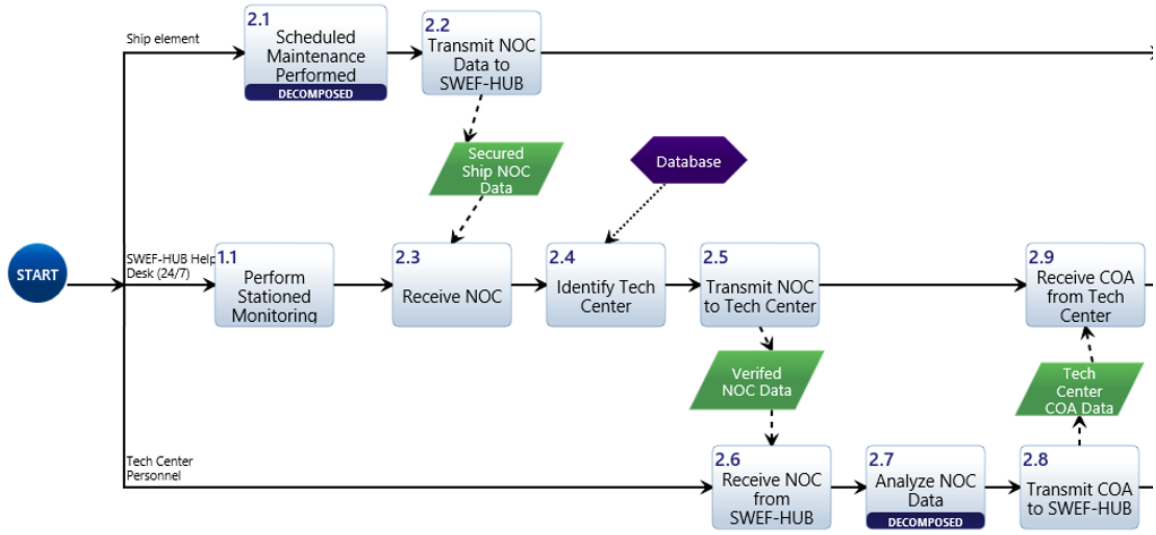


Figure 26. Condition-Based Maintenance (CBM) Near-Term Action Diagram, Part A

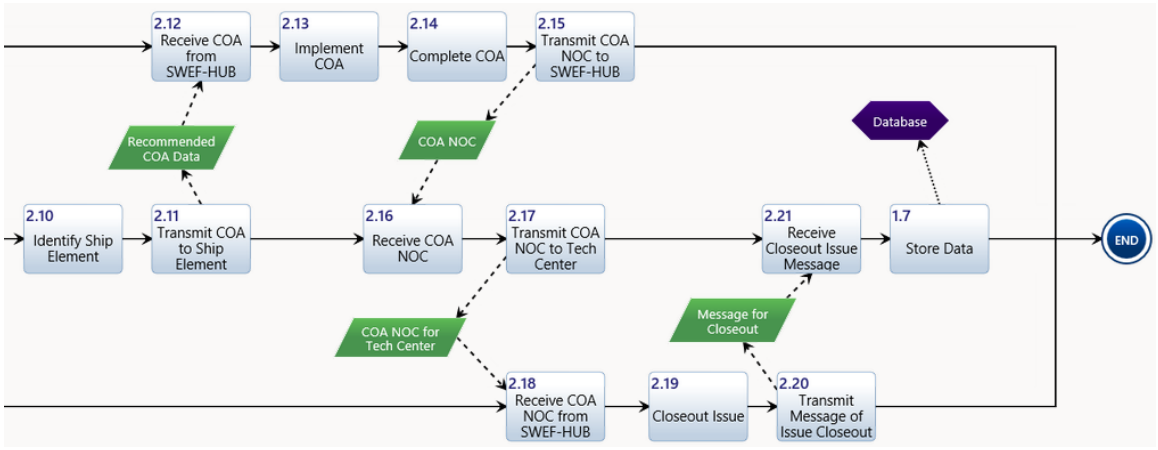
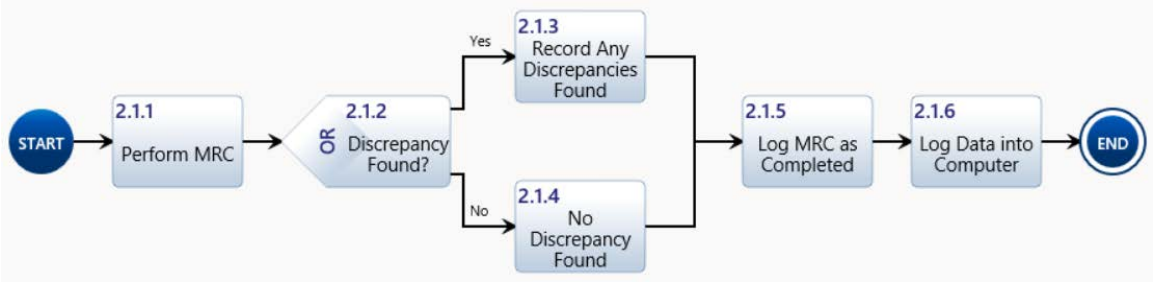


Figure 27. Condition-Based Maintenance Near-Term Action Diagram, Part B

a. Condition-Based Maintenance Near-Term Action Diagram Description. (Scheduled Maintenance Decomposed Diagram)

The regularly scheduled maintenance performed by the ship element, shown in Figure 28, starts with the performance of the maintenance requirement card (MRC), action (2.1.1). After performing the MRC, a decision point is reached (2.1.2). If any discrepancies are found, they are recorded (2.1.3). Once the discrepancy data is recorded or if no discrepancies are found (2.1.4), the MRC is logged as complete (2.1.5) and the data is stored (2.1.6).



(2.1.1)

Figure 28. Condition-Based Maintenance Near-Term Action Diagram, 2.1.

b. Condition-Based Maintenance Near-Term Action Diagram Description. (Analyze NOC Data Decomposed Diagram)

Personnel at the appropriate technical center perform the analysis of the NOC data as shown in Figure 29. The NOC data is checked for anomalies, action (2.7.1). After checking the data, the technical center reaches a decision point (2.7.2). If they detect an anomaly, they examine it (2.7.3) and identify it (2.7.4). Once identified, they determine whether to assign a corrective or preventive maintenance action (2.7.5). If the technical center determines a maintenance action, or if they detect no anomalies (2.7.6), they provide a COA (2.7.7)

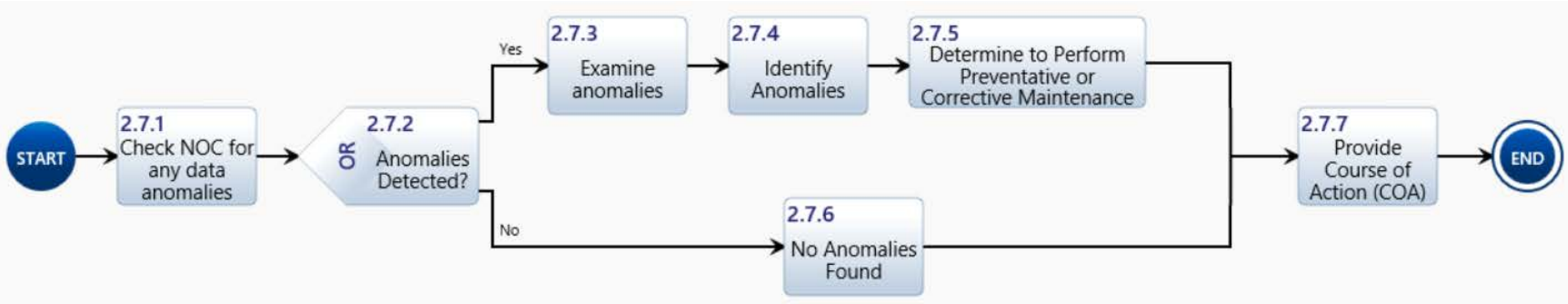


Figure 29. Condition-Based Maintenance Near-Term Action Diagram, 2.7

3. Raw Data Collection Near-Term Action Diagram (and Scheduled Maintenance Decomposed Diagram) Description

As indicated in Figure 30, the raw data collection near-term action process contains two elements: the ship element and the SWEF-Hub help desk. The ship element performs the scheduled maintenance, action (2.1), and then sends a secured email to the SWEF-Hub stating that the maintenance action is complete (2.2). The SWEF-Hub receives (2.3), reviews (3.4), categorizes (1.6), and stores the maintenance history data (1.7) in the database. The SWEF-Hub is manned 24/7, the personnel are biometrically authenticated, and its operational status is continuously monitored (1.1).

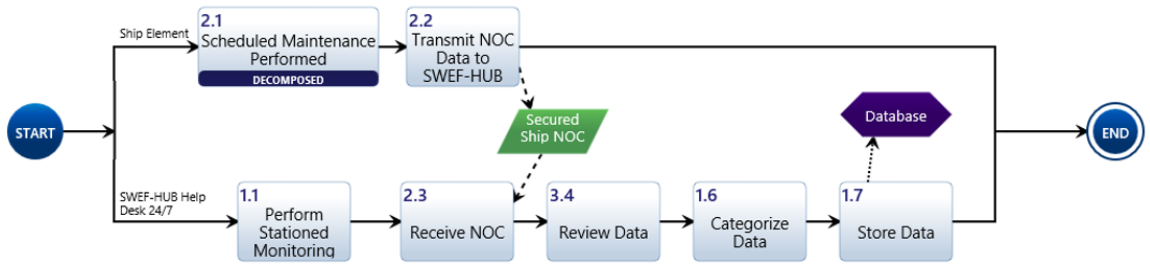


Figure 30. Raw Data Collection Near-Term Action Diagram

The raw data collection near-term action diagram shown in Figure 30 contains a scheduled maintenance performed action (2.1). Action (2.1) is decomposed and described in Chapter V Section D paragraph 5.a and shown in Figure 28.

4. Troubleshooting Near-Term Action Description

The troubleshooting near-term action process contains three elements: the ship element, the SWEF-Hub help desk, and technical center personnel. Figure 31 shows the entire process, while Figures 32 and 33 show the details. When the ship element detects an issue with one of the combat systems, action (4.1), it generates and securely sends an email to the SWEF-Hub help desk (4.2). The SWEF-Hub is manned 24/7, the personnel are biometrically authenticated, and its operational status is continuously monitored (1.1). It receives the casualty data (4.3), analyses it (4.4), and stores it in the database. Once the SWEF-Hub determines the appropriate technical center (2.4), it sends a notification to the

technical center. The technical center receives the notification data (4.5), analyses it for anomalies (4.6), troubleshoots as necessary (4.7), and develops a solution (4.8); action (4.8) is shown decomposed in Chapter V Section D paragraph 4.a below and illustrated in Figure 34. The technical center securely sends the COA data to the SWEF-Hub help desk. The SWEF-Hub help desk receives the recommended solution (4.9) and passes it to the ship element. The ship element receives the solution (4.10), then implements the solution (4.11). If this action resolves the issue (4.12), a NOC is developed (4.14). If the implemented solution does not fix the problem, troubleshooting continues until the issue is resolved (4.13), followed by development of a NOC (4.14). The ship element sends the COA NOC to the SWEF-Hub. The SWEF-Hub receives the NOC (2.3), identifies the appropriate technical center (2.4), and sends the NOC to the technical center. The technical center receives the NOC (4.15), reviews it (4.16), and stores it in the database. Next, the technical center closes out the issue (2.19) and transmits the closeout message to the SWEF-Hub (2.20). The SWEF-Hub receives the closeout message (2.21) and stores the repair data in the database (1.7).

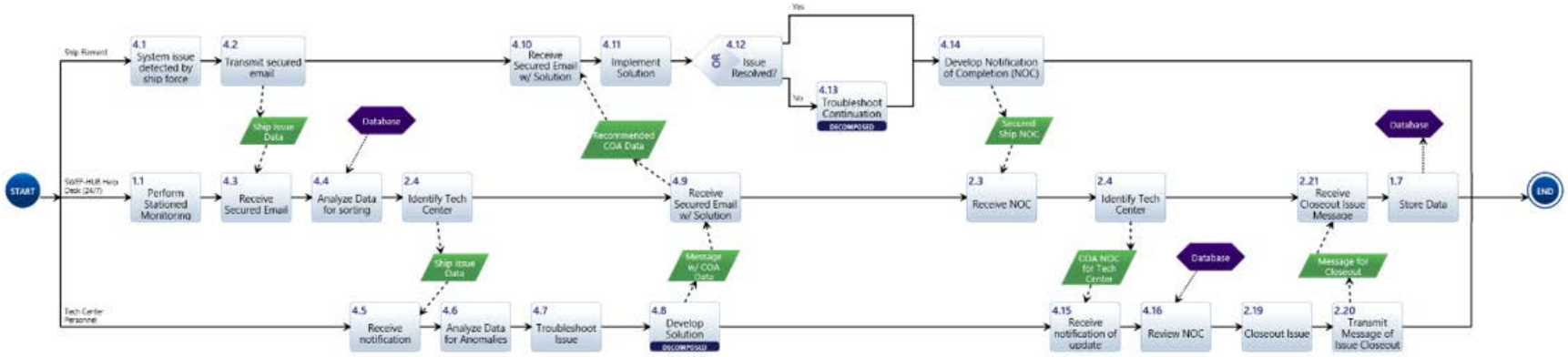


Figure 31. Troubleshooting Near-Term Action Diagram

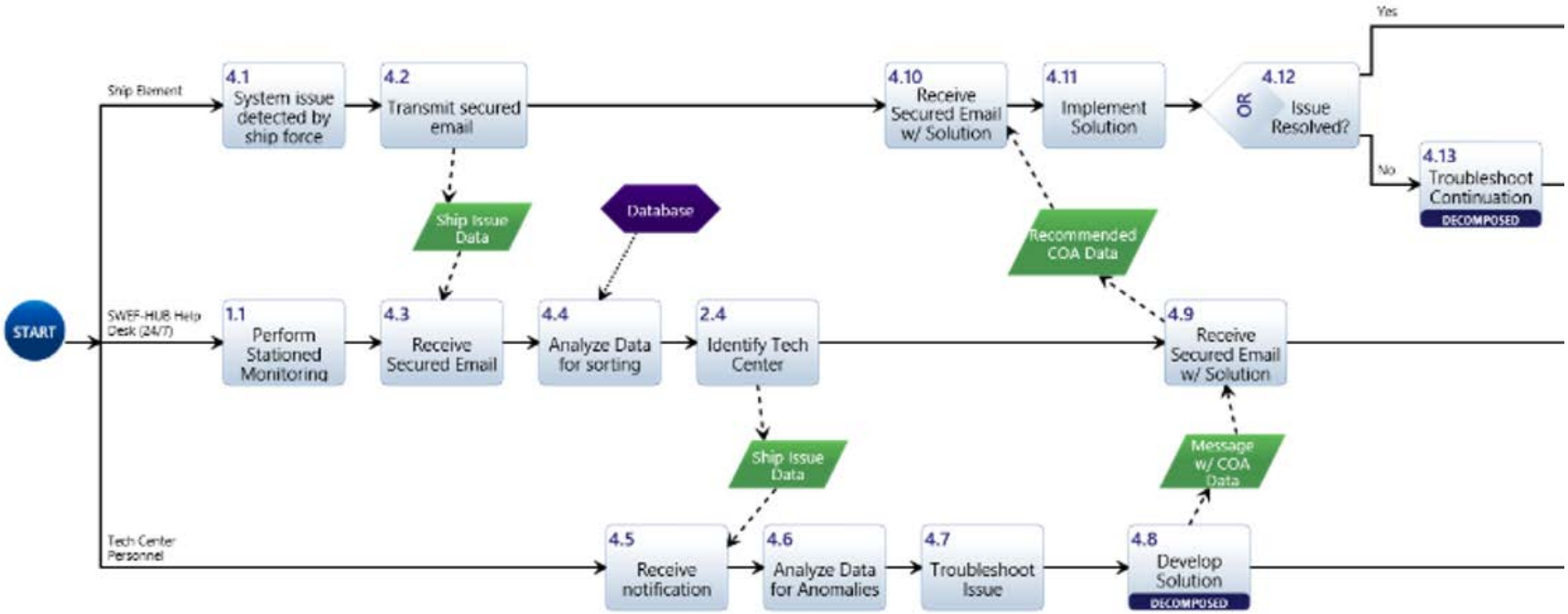


Figure 32. Troubleshooting Near-Term Action Diagram, Part A

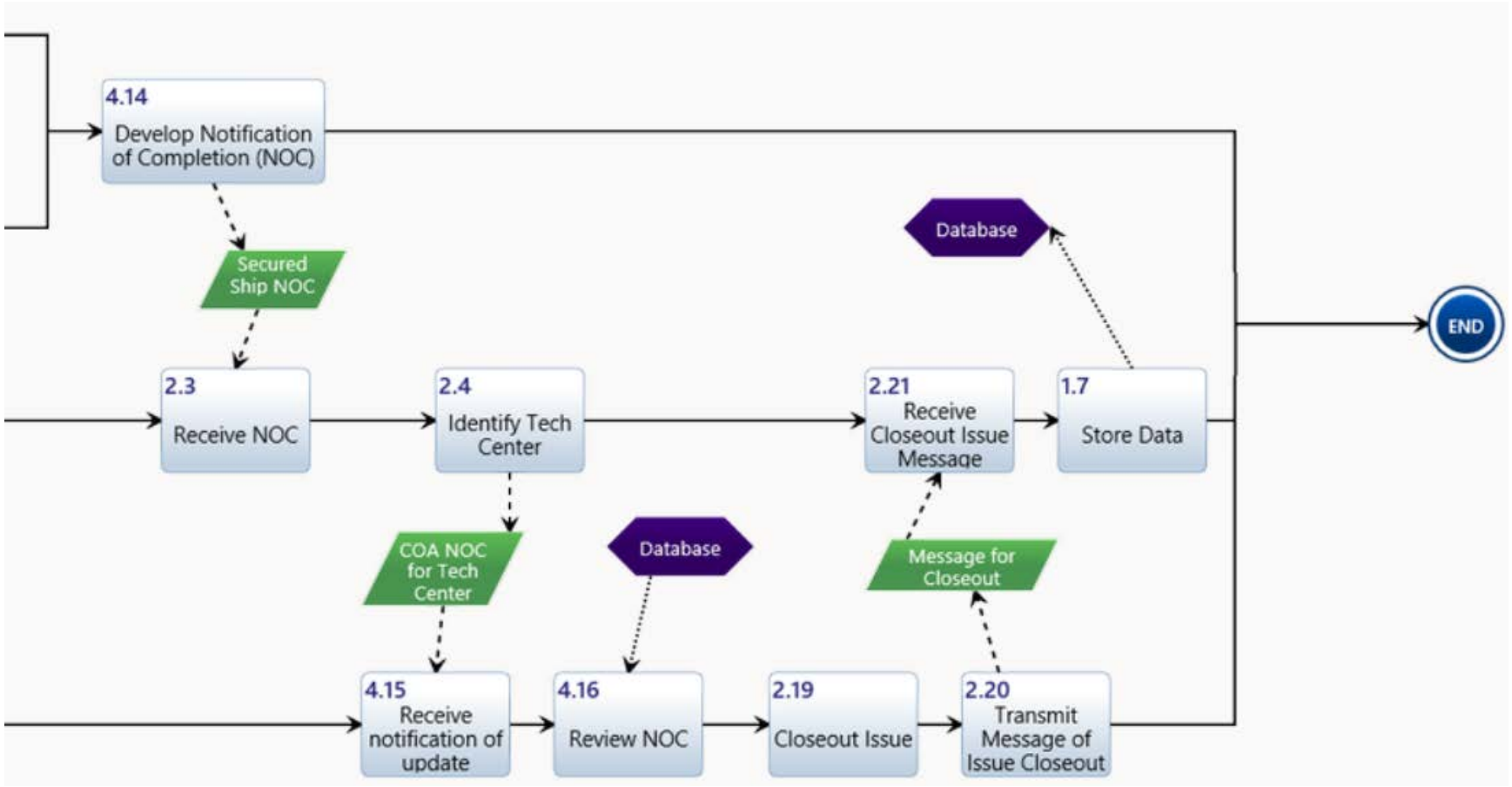


Figure 33. Troubleshooting Near-Term Action Diagram, Part B

a. Troubleshooting Near-Term Action Diagram Description (Troubleshoot/ Solution Decomposed Diagram)

As indicated in Figure 34, this sub-process starts with the ship element reviewing past data for a solution to a similar issue, action (4.8.1). After the ship element reviews past data, it reaches a decision point (4.8.2). If the ship element found a solution (4.8.8), the solution is sent to the SWEF-Hub (4.8.9). If it did not find a solution, then another decision point is reached (4.8.3). If a solution is not developed remotely, personnel are sent to troubleshoot the issue (4.8.4). If the issue is developed remotely, troubleshooting occurs (4.8.5). This triggers another decision point (4.8.6). If the issue is not resolved, continue troubleshooting until it is resolved (4.8.7). If the issue is resolved, the solution is sent to the SWEF-Hub (4.8.9).

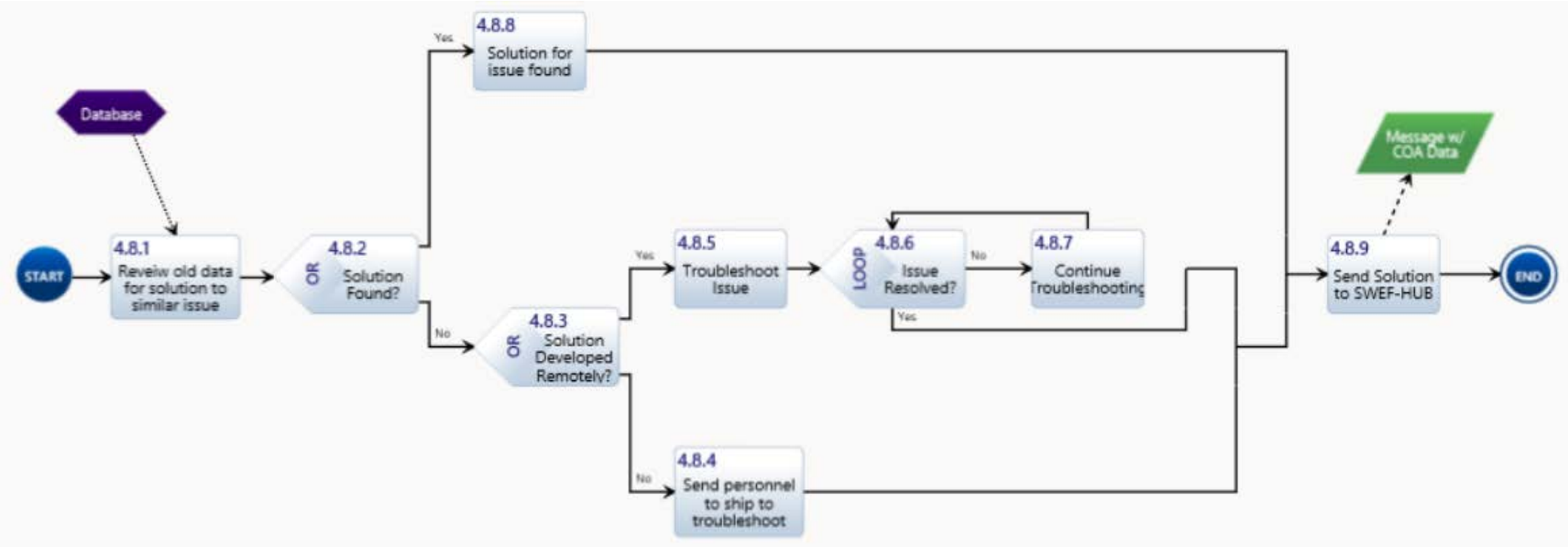


Figure 34. Troubleshooting Near-Term Action Diagram, 4.8

b. Troubleshooting Near-Term Action Diagram Description (Develop Solution Decomposed Diagram)

As indicated in Figure 35, this sub-process starts in the technical center with a decision point, action (4.13.1). When the technical center resolves the issue, the sub-process ends. Otherwise, the technical center continues to troubleshoot the issue until a solution is found (4.13.2).

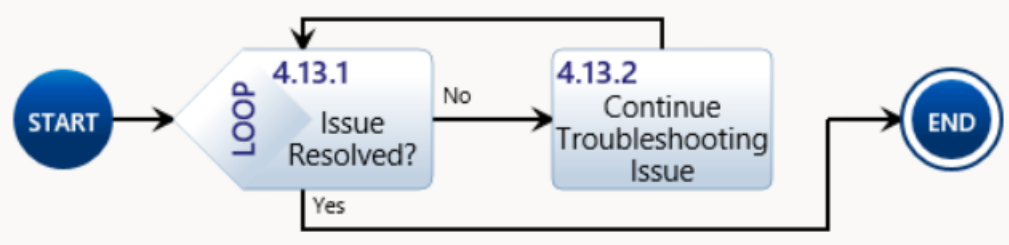


Figure 35. Troubleshooting Near-Term Action Diagram, 4.13

5. Software Upgrade Near-Term Action Diagram Description

The software upgrade near-term action process contains three elements: the ship element, the SWEF-Hub help desk, and the technical center personnel. Figure 36 shows the process. The technical center personnel develop a software upgrade or patch, action (5.1), then securely sends it to the SWEF-Hub (5.2). The SWEF-Hub is manned 24/7, the personnel are biometrically authenticated, and its operational status is continuously monitored (1.1). The SWEF-Hub receives the software upgrade or patch (5.3) and stores the software data in the database. The SWEF-Hub analyzes the software to determine the distribution (5.4) and identify the appropriate ship element (5.5) using the information stored in the database. Once the SWEF-Hub identifies the ship element, the SWEF-Hub sends out the software upgrade or patch to the ship element. The ship element receives (5.6) and implements the software upgrade or patch (5.7). Upon completion of the action, the ship element sends a NOC to the SWEF-Hub (5.8). The SWEF-Hub receives the NOC (2.3) and stores the NOC data (1.7) in the database. The SWEF-Hub forwards the NOC to the technical center personnel (5.9). The technical center personnel receive the NOC (2.3).

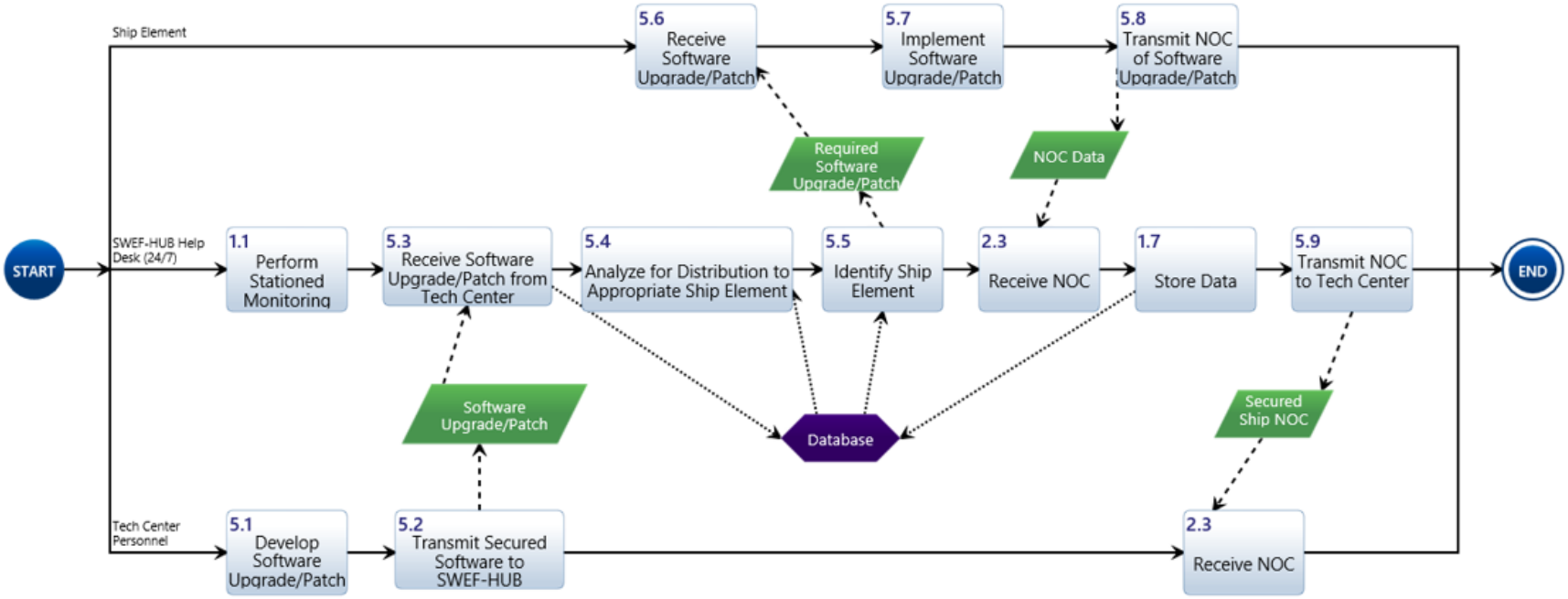


Figure 36. Software Upgrade Near-Term Action Diagram

6. Secondary Collaboration Near-Term Action Diagram (and Determination of Requirements for Testing Decomposed Diagram) Description

The secondary collaboration near-term action diagram process has three elements: the system element, the SWEF-Hub help desk, and the technical center personnel. Figure 37 shows the entire process, while Figures 38, 39, and 40 show the details. The system element sends a secured email request to the SWEF-Hub help desk, action (6.1). The SWEF-Hub is manned 24/7, the personnel are biometrically authenticated, and its operational status is continuously monitored (1.1). The help desk receives (6.2) and processes the request (6.3). It then uses the database to identify the appropriate technical center (6.4) and routes the request to that center (6.5). The technical center receives (6.6), approves (6.7) and sends the approved request back to the SWEF-Hub help desk (6.8). The SWEF-Hub receives the approval (6.9), sends the approval to the system element (6.10) and the system element receives the approval (6.11). A technician travels to the SWEF-Hub to set up the system (6.13) and prepares the SWEF-Hub for a simulated test environment (6.14), triggering the system element to send the data needed for simulation to the SWEF-Hub (6.12). The SWEF-Hub receives the data (6.15), implements the data into the simulated test environment (6.16), and stores the system simulation data in the database. The SWEF-Hub runs the simulation (6.17), records the results (6.18), and stores the simulation results data (1.7) in the database. The SWEF-Hub sends the results from the database to the system element (6.19). The system element receives the results (6.20).

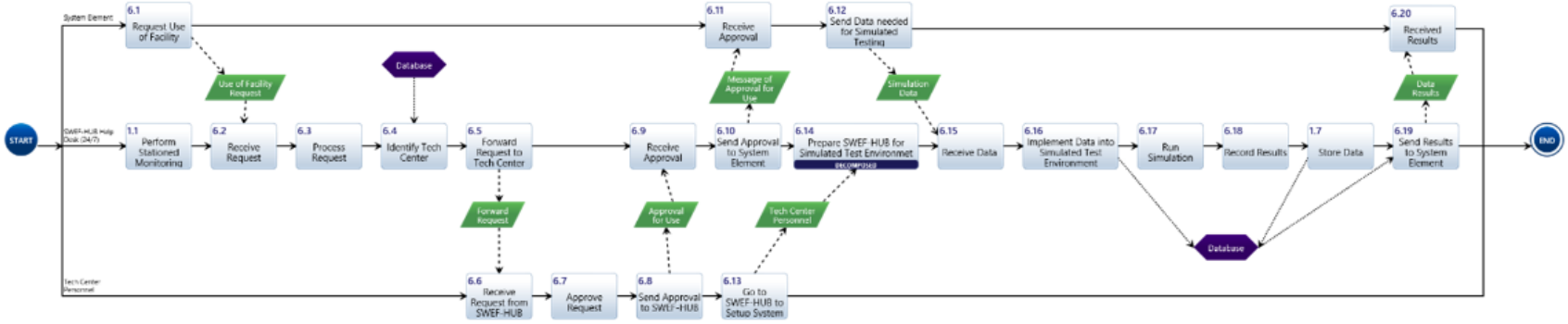


Figure 37. Secondary Collaboration Near-Term Action Diagram

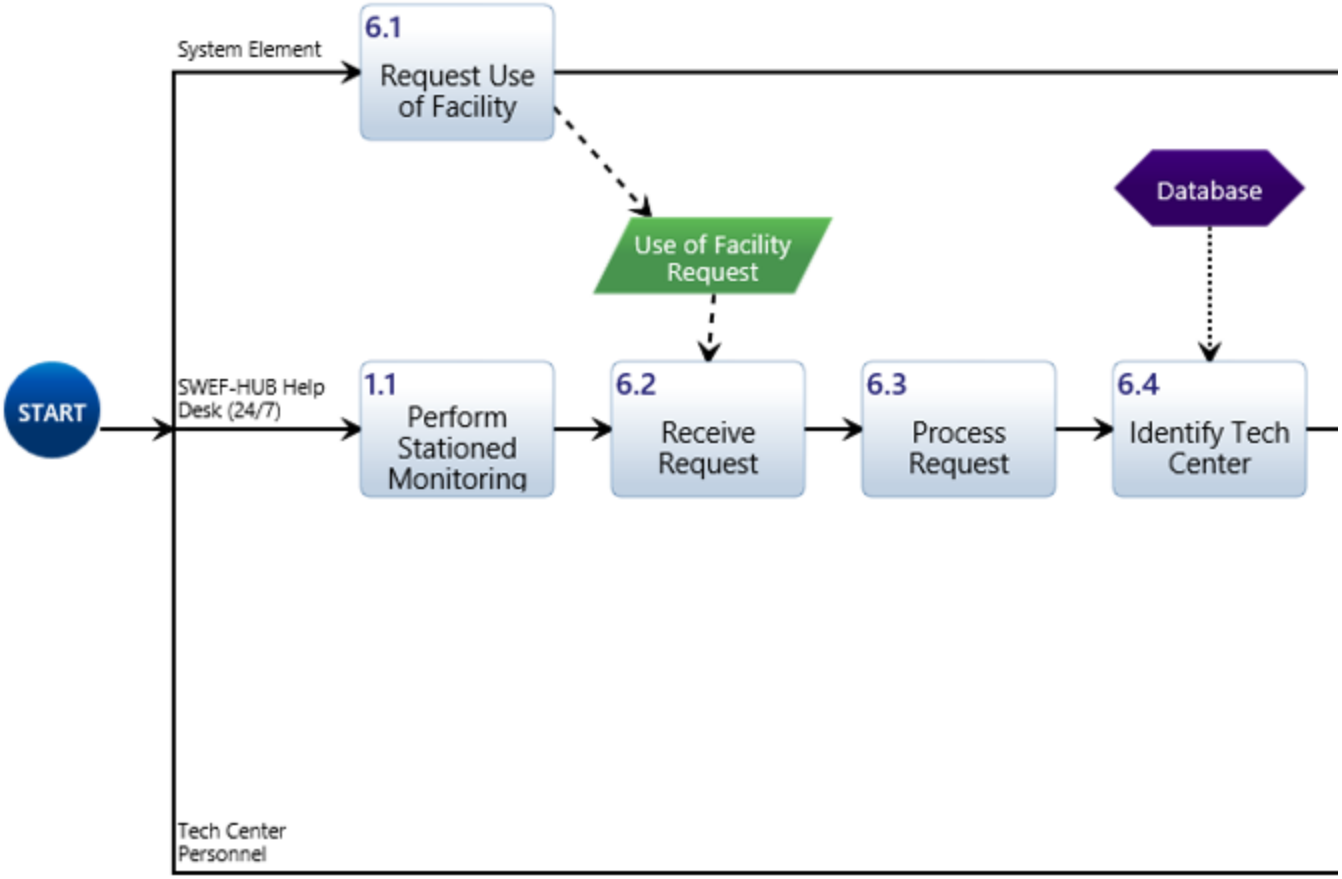


Figure 38. Secondary Collaboration Near-Term Action Diagram, Part A

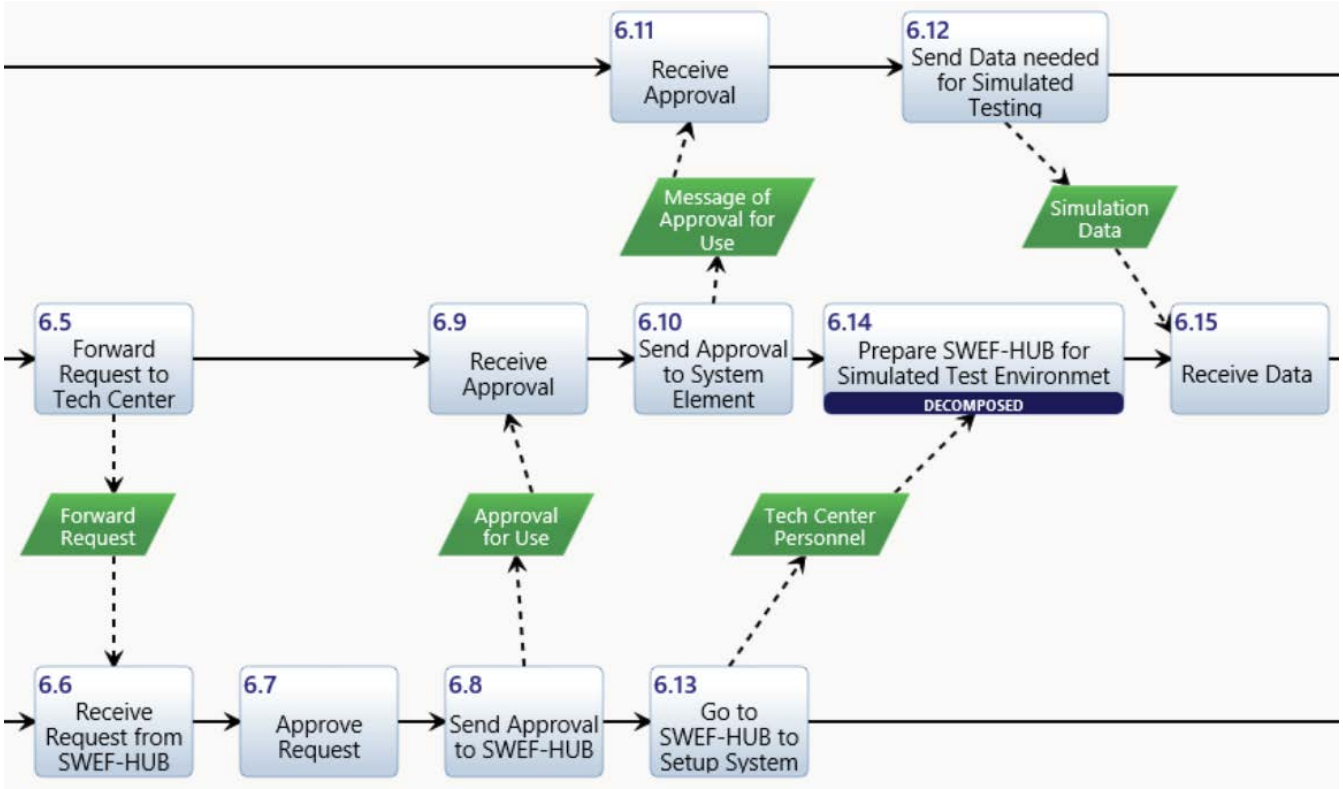


Figure 39. Secondary Collaboration Near-Term Action Diagram, Part B

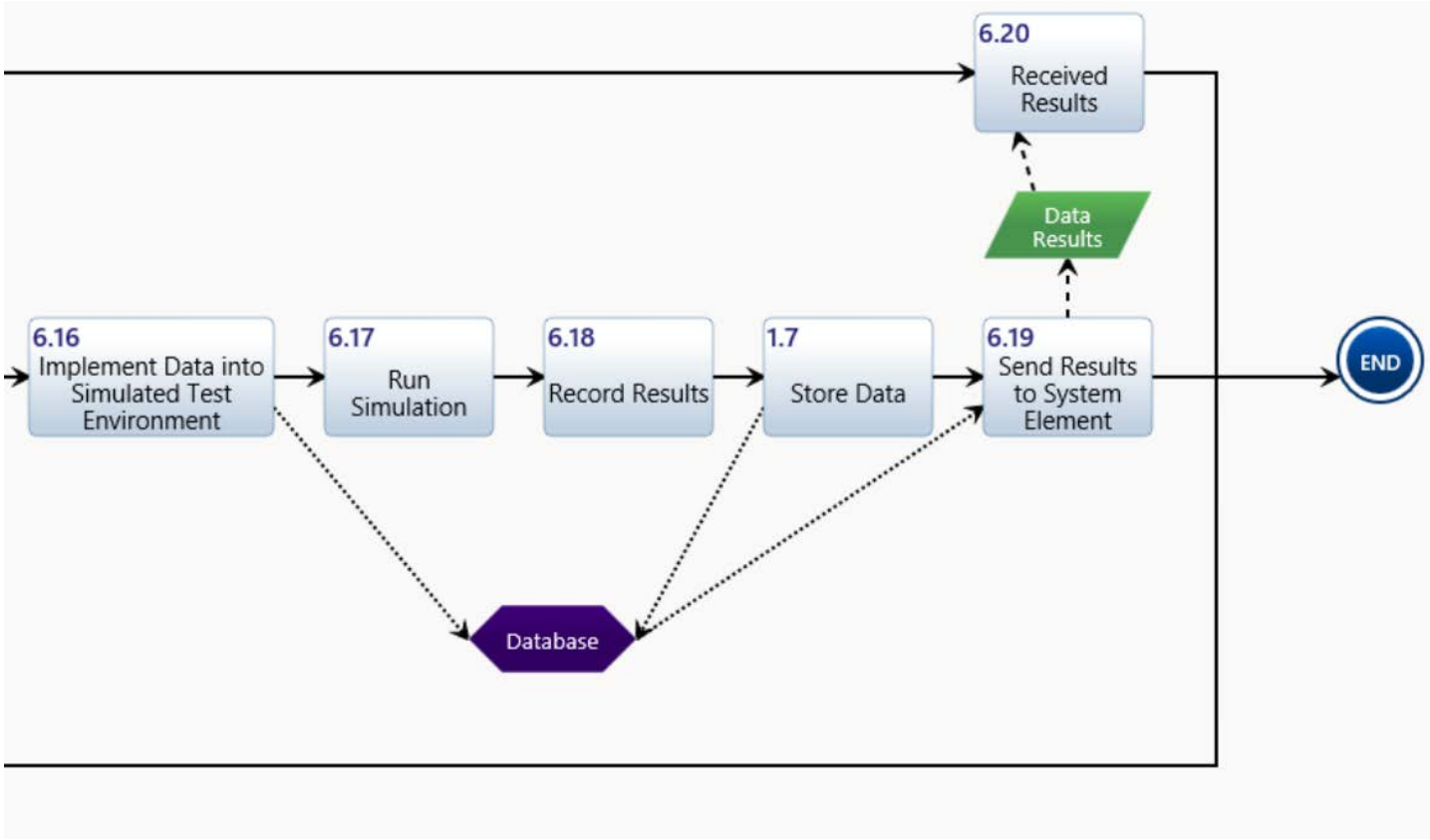


Figure 40. Secondary Collaboration Near-Term Action Diagram, Part C

The secondary collaboration near-term action diagram (determination of requirements for testing decomposed diagram) is described next. As indicated in Figure 41, this sub-process starts when technical center personnel travel to the SWEF-Hub help desk to determine the hardware requirements for testing, action (6.14.1). After establishing the hardware requirements, the technical center personnel determine the software requirements (6.14.2). Next, they determine the system layout (6.14.3) and set up the required system (6.14.4).

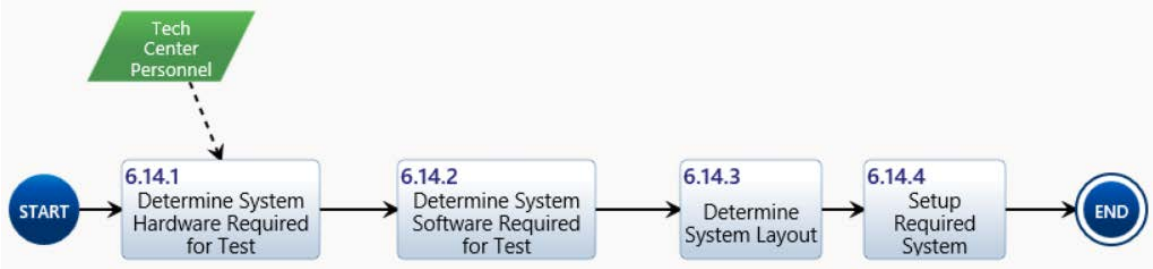


Figure 41. Secondary Collaboration Near-Term Action Diagram, 6.14

E. LONG-TERM FUNCTIONAL ARCHITECTURE

Long-term architecture defines an architecture that will be implemented approximately ten years in the future. It encompasses a machine learning system that utilizes different databases and tools to provide long distance support in real time.

The following diagrams illustrate the long-term architecture:

1. Combat Systems Health Long-Term Action Diagram Description

As indicated in Figure 42, the combat systems health near-term action process contains two elements: the ship element and the SWEF-Hub element. The SWEF-Hub element contains two sub-elements: the ML program that has an automated data process and personnel who operate and monitor the SWEF-Hub.

The ship element has an automated data query. Once the data is “pulled,” action (7.1), the ship element secures the data using an automated process (7.2) and sends it to the SWEF-Hub (7.3). At the SWEF-Hub, the ML program receives the data (7.4) and analyzes

it using information from the database (7.5). The ML program then categorizes the data (7.6) and stores the data (7.7) into the database using automated processes. The SWEF-Hub is manned 24/7, the personnel are biometrically authenticated, and its operational status is continuously monitored (1.1).

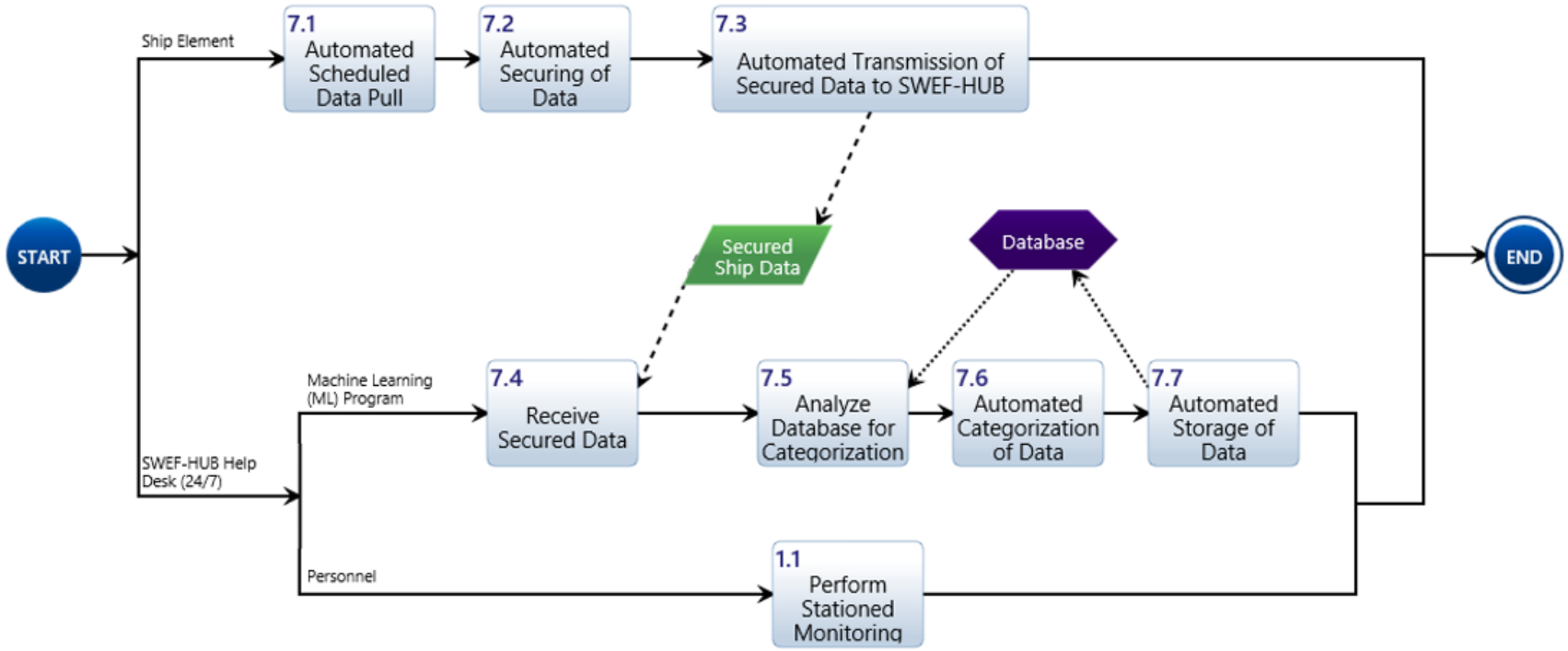


Figure 42. Combat Systems Health Long-Term Action Diagram.

2. Condition-Based Maintenance Long-Term Action Diagram Description

The long-term CBM process action diagram uses the same three elements used in the near-term CBM process, but in this case, the SWEF-Hub help desk has two sub-elements: the ML program and SWEF-Hub personnel. The entire process is shown in Figure 43 as a visual reference only, while the details are shown in Figures 44, 45, 46, and 47. Starting with the ship element, onboard maintenance personnel execute equipment maintenance actions that are automatically scheduled, action (2.1); action (2.1) is shown decomposed in Chapter V Section E paragraph 2.a below and illustrated in Figure 48. When the action is completed, the NOC data is securely emailed to the ML program of the SWEF-Hub help desk (2.2).

The SWEF-Hub is manned 24/7, the personnel are biometrically authenticated, and its operational status is continuously monitored (1.1). After the ML system element receives the NOC data (2.3), it automatically stores the maintenance data in the database (7.7). The ML system element utilizes the database and performs initial analyses using automated processes (8.1); action (8.1) is shown decomposed in Chapter V Section E paragraph 2.b below and illustrated in Figure 49. The ML system element uses the database to identify the appropriate technical center (8.2), then prepares and sends a notification message to the personnel side of SWEF-Hub (8.3). The SWEF-Hub personnel analyze the message for accuracy (8.4); action (8.4) is shown decomposed in Chapter V Section E paragraph 2.c below and illustrated in Figure 52. The SWEF-Hub personnel forward the message with COA to the appropriate technical center (8.5). Subject matter experts within the technical center receive (8.6) and analyze the COA determined by the ML program (8.7); action (8.7) is shown decomposed in Chapter V Section E paragraph 2.d below and illustrated in Figure 53. The subject matter experts approve the recommended or adjusted COA (8.8), and the message with COA is sent back to the SWEF-Hub (8.9). The SWEF-Hub receives the message (8.6) and loads and stores this data/COA into the ML program (8.10), storing the data and COA message in the database. The ML program receives (8.11) and analyzes the COA data (8.12). Following this ML analysis, the SWEF-Hub utilizes the database to identify the ship element (8.13) and transmits the recommended COA to the

ship element (8.14). The ship element receives the recommended COA (8.15) and implements it (8.16). Upon completion of the COA (8.17), the ship element generates and sends a COA NOC to the SWEF-Hub (8.18). The ML program of SWEF-Hub receives the NOC (8.19), stores the NOC data using an automated process (7.7) into the database, and utilizes the database to identify the technical center (6.4). The ML program transmits a confirmation message for delivery to personnel in the SWEF-Hub (8.20). When the personnel side of the SWEF-Hub receives the message (8.6), they confirm it and send the COA NOC to the appropriate technical center (8.21). The technical center receives the COA NOC (8.22), closes it (2.19), and sends a closeout message back to the ML program of the SWEF-Hub (for storage) (2.20). When the ML program receives the closeout message (2.21), it stores the closeout data in the database (7.7).

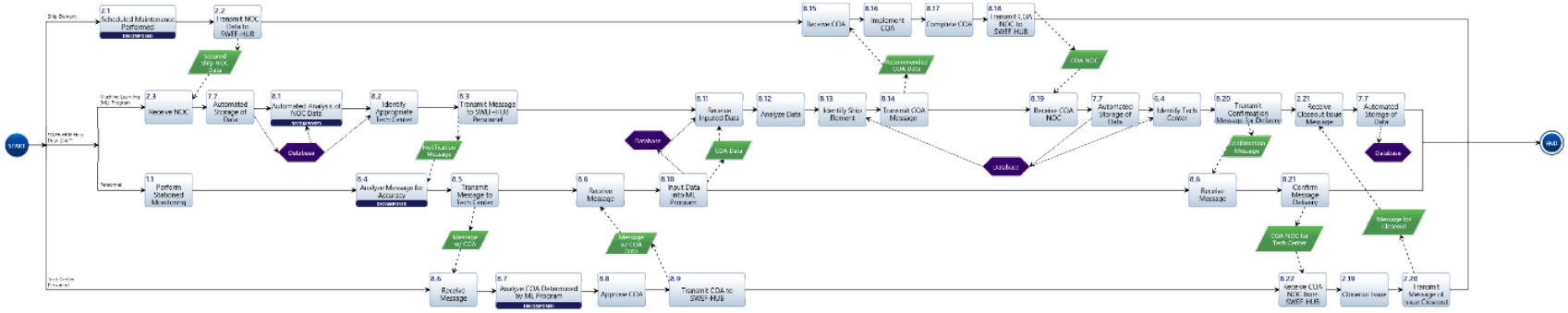


Figure 43. Condition-Based Maintenance Long-Term Action Diagram

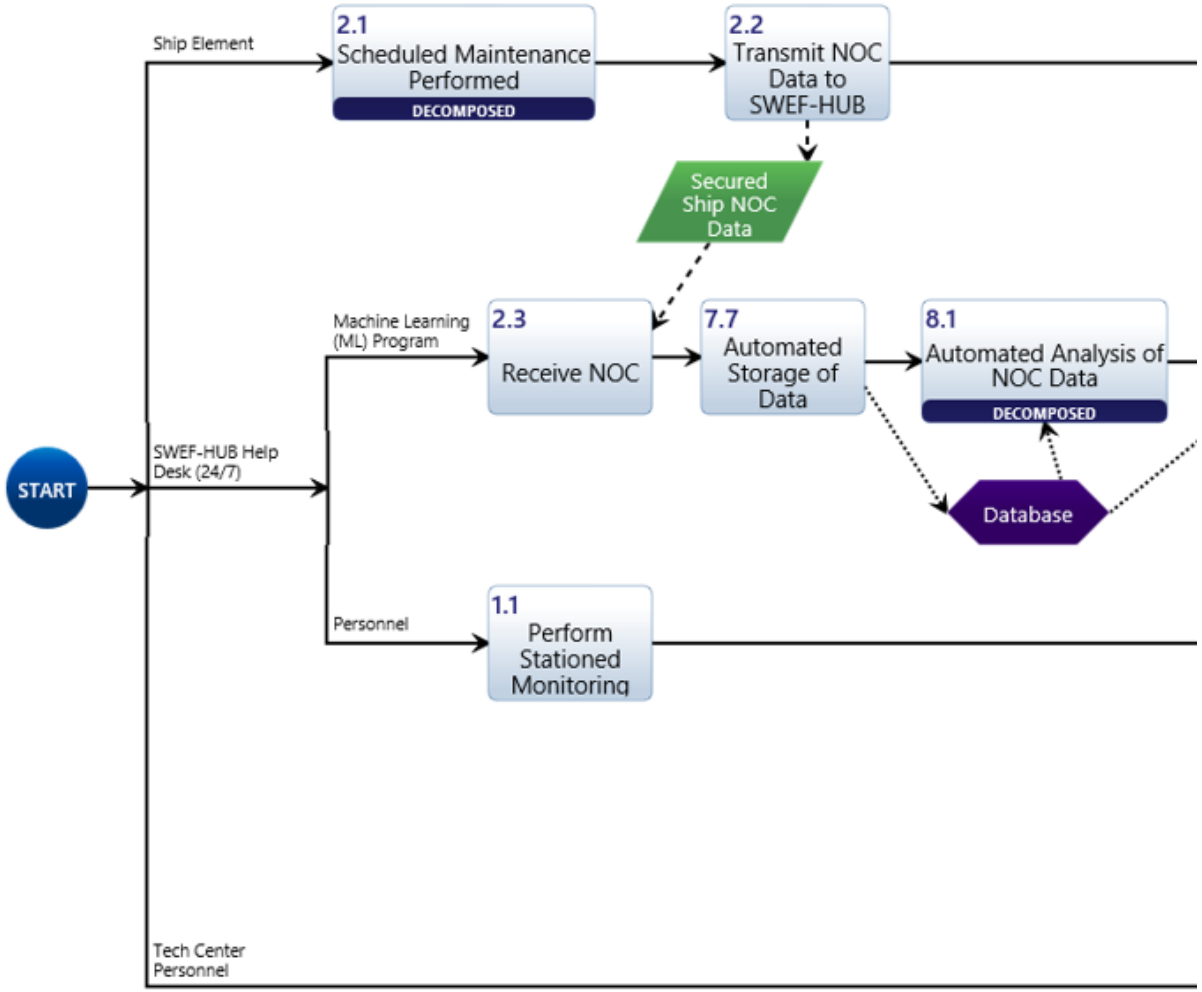


Figure 44. Condition-Based Maintenance Long-Term Action Diagram, Part A

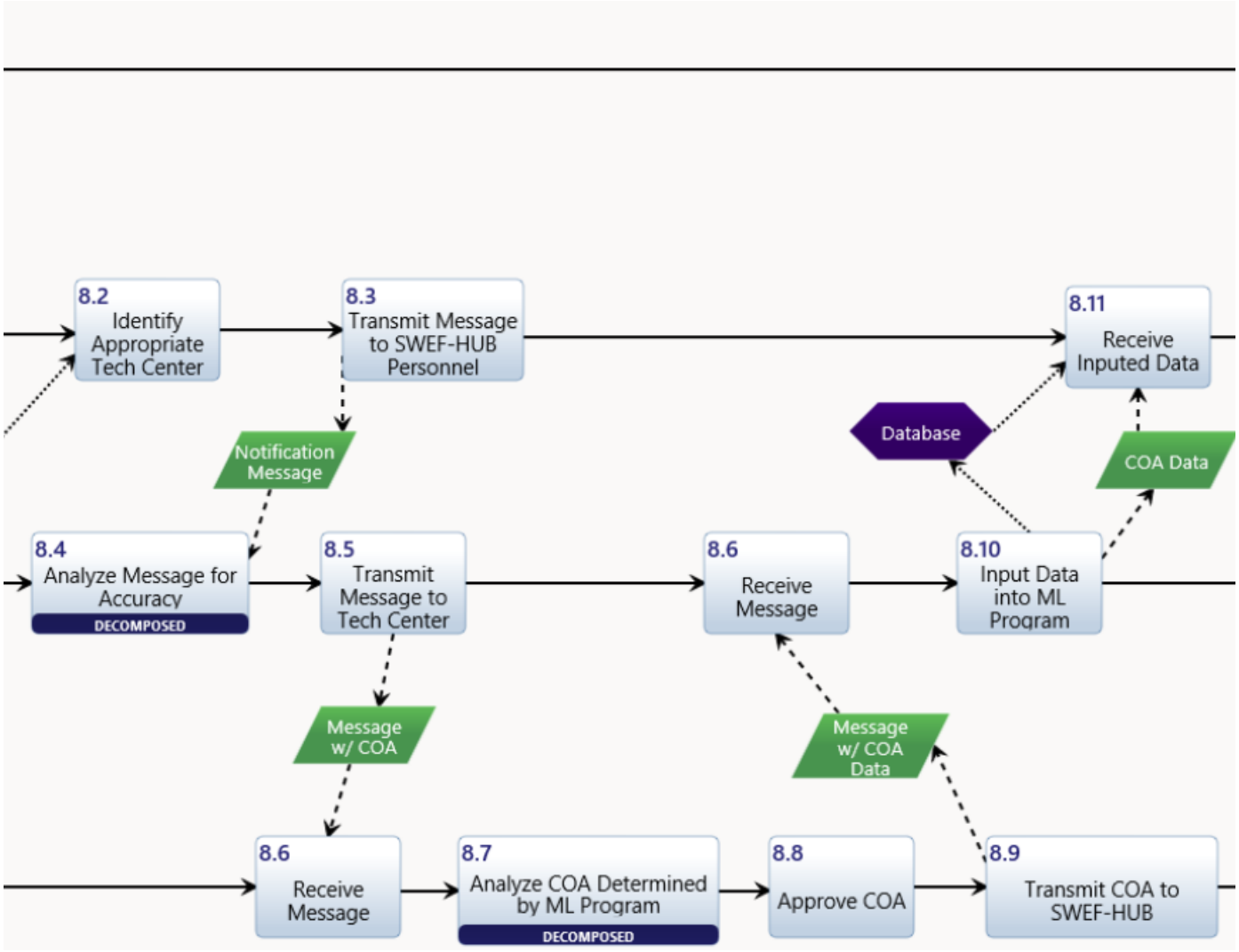


Figure 45. Condition-Based Maintenance (CBM) Long-Term Action Diagram, Part B

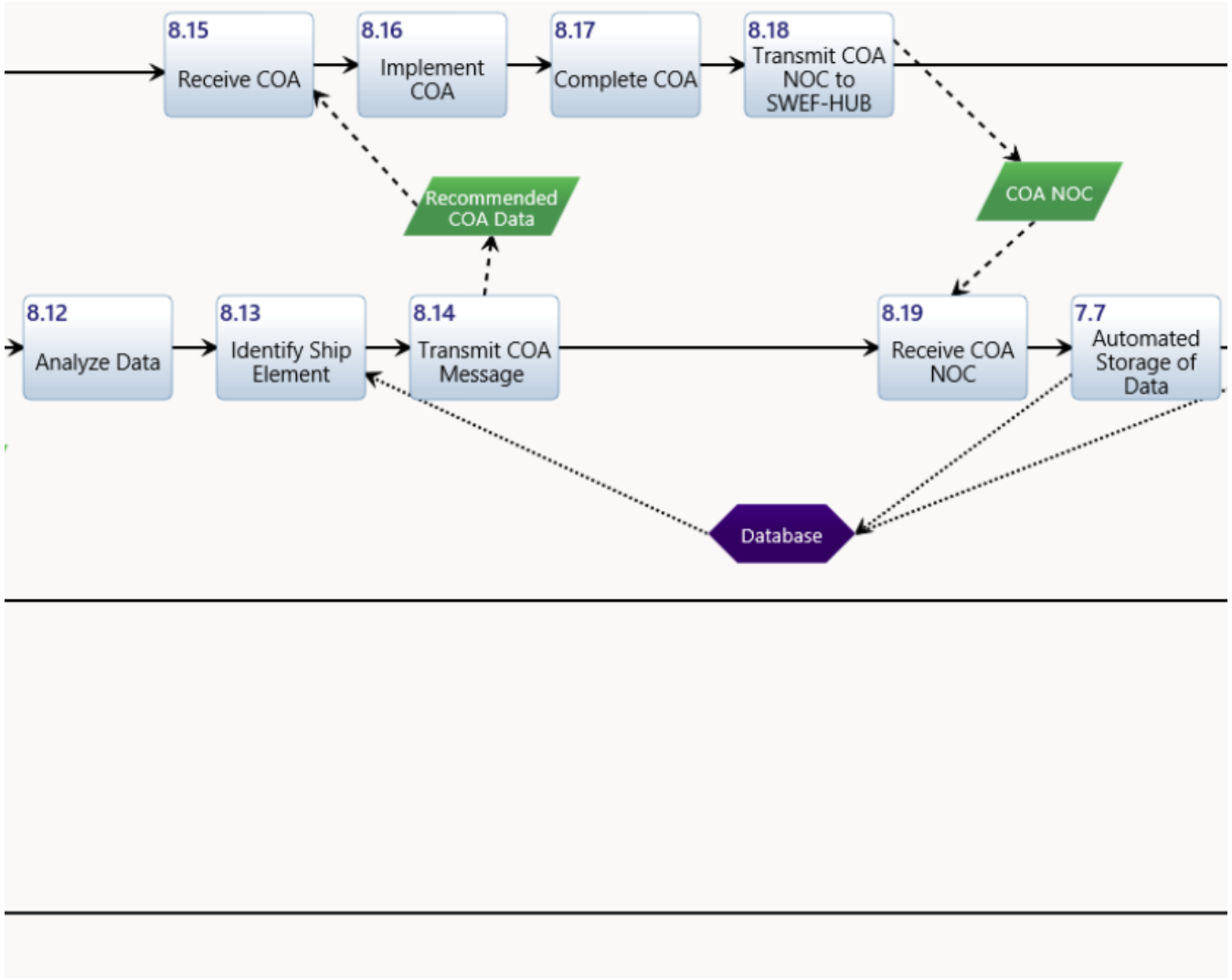


Figure 46. Condition-Based Maintenance Long-Term Action Diagram, Part C

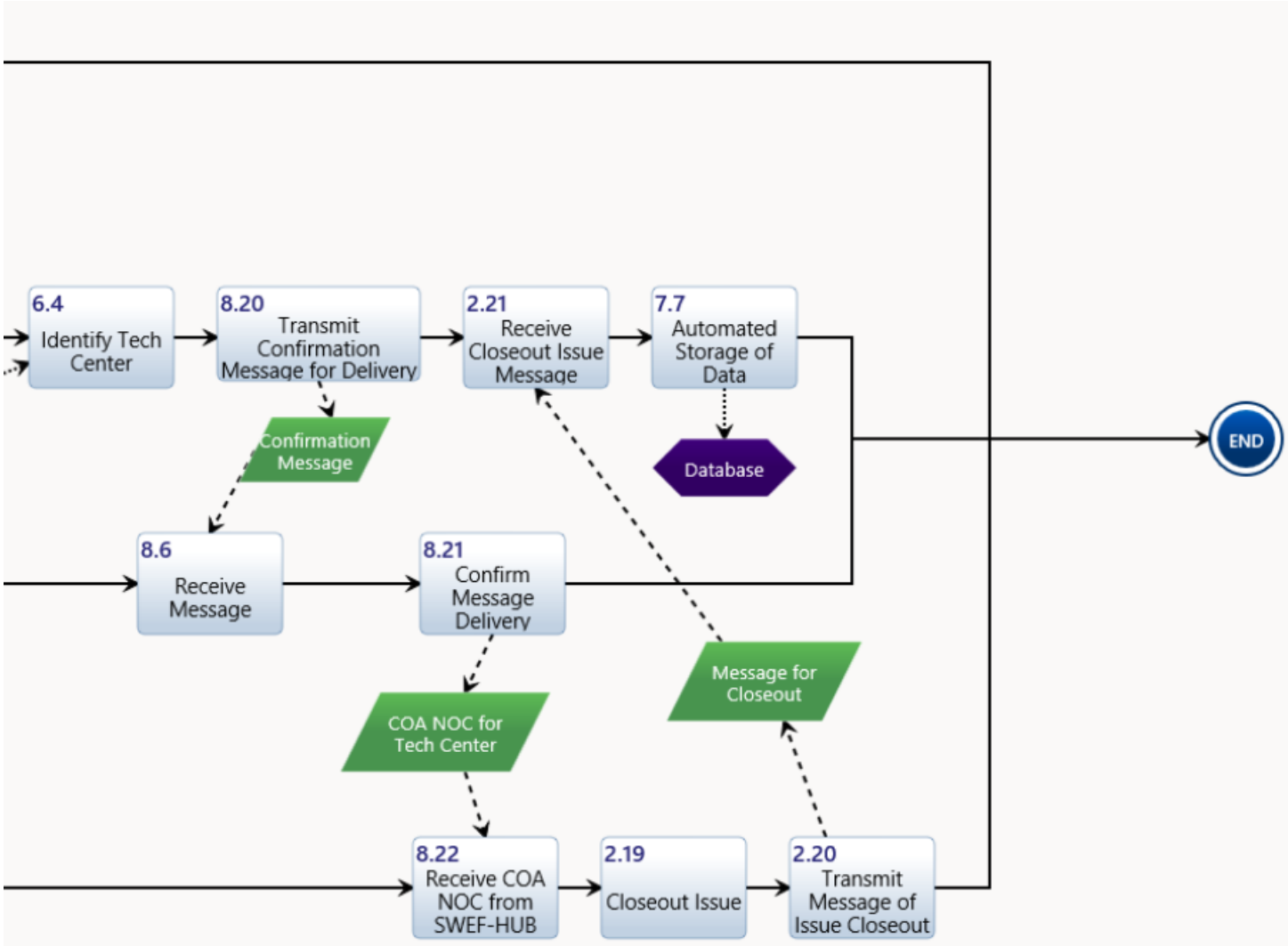


Figure 47. Condition-Based Maintenance Long-Term Action Diagram, Part D

a. Condition-Based Maintenance Long-Term Action Diagram Description (Scheduled Maintenance Decomposed Diagram)

As indicated in Figure 48, the regularly scheduled maintenance performed by the ship element starts with the performance of the maintenance requirement card (MRC), action (2.1.1). After the MRC is performed, a decision point is reached (2.1.2). If any discrepancies are found, they are recorded (2.1.3). After the discrepancies are recorded or if no discrepancies are found (2.1.4), the ship element logs the MRC as complete (2.1.5) and logs the data into a computer for storage (2.1.6).

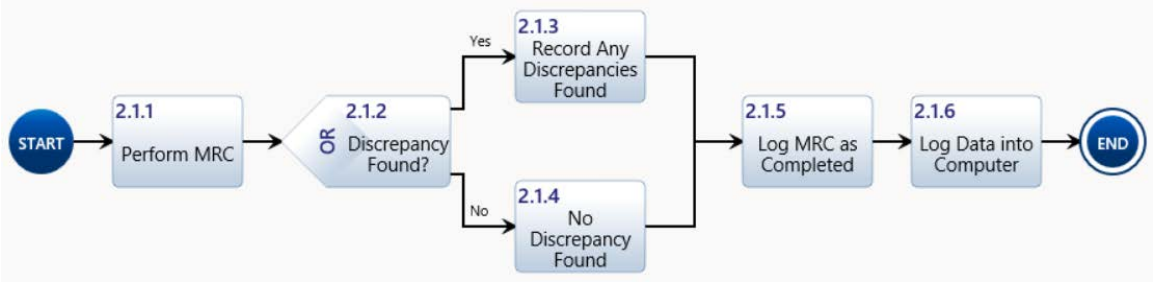


Figure 48. Condition-Based Maintenance Long-Term Action Diagram, 2.1.

b. Condition-Based Maintenance Long-Term Action Diagram Description (Analyze NOC Data Decomposed Diagram)

Figure 49 shows the entire process for a visual reference only, while Figures 50 and 51 show the details of the process. The ML program of the SWEF-Hub help desk analyzes the database for normal system condition settings, action (8.1.1). It checks the NOC data for anomalies by comparing the data against normal system conditions in the database, action (8.1.2). After checking the data, a decision point is reached (8.1.3). If the ML program detects an anomaly, the ML program examines it further (8.1.4) and reviews the database for a documented course(s) of action (COA) (8.1.5) previously used to resolve the anomalous condition. When the ML program finishes its analysis of the database, another decision point is reached (8.16). Depending on whether the ML program found a preventative or corrective COA, it generates either a preventative COA (8.1.7), a corrective COA (8.1.8), or no maintenance detected COA (8.1.9). If the ML system found no

anomalies, it documents that no anomalies were detected (8.1.10). At the end of the process, a final course of action (COA) is provided (8.1.11).

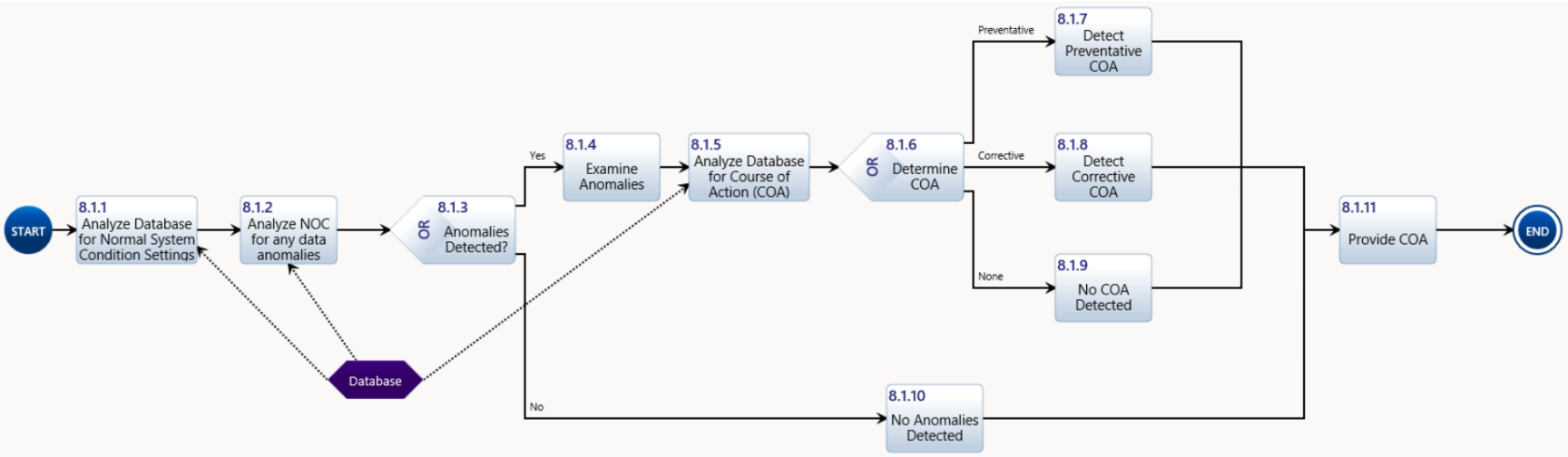


Figure 49. Condition-Based Maintenance Long-Term Action Diagram, 8.1

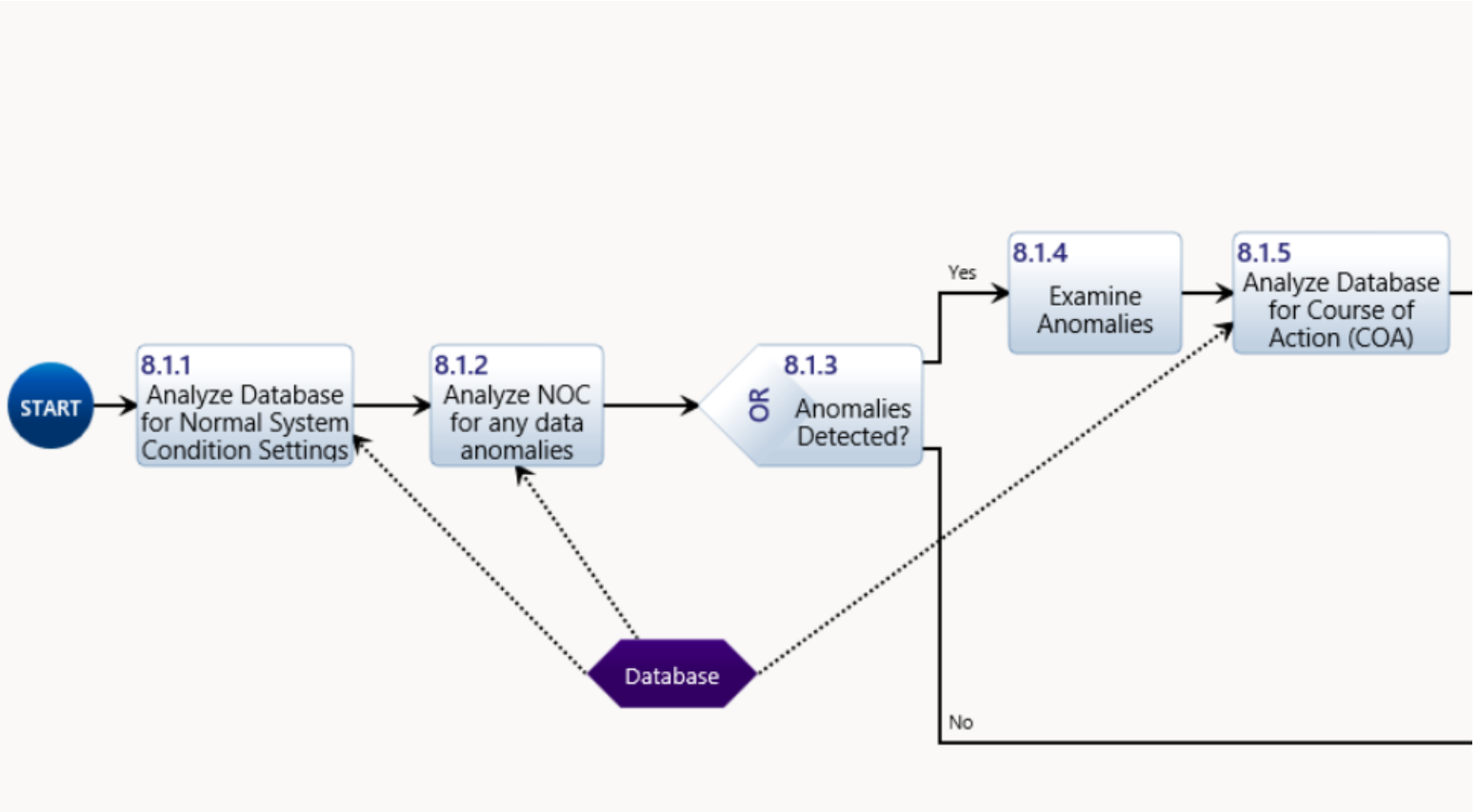


Figure 50. Condition-Based Maintenance Long-Term Action Diagram, 8.1, Part A

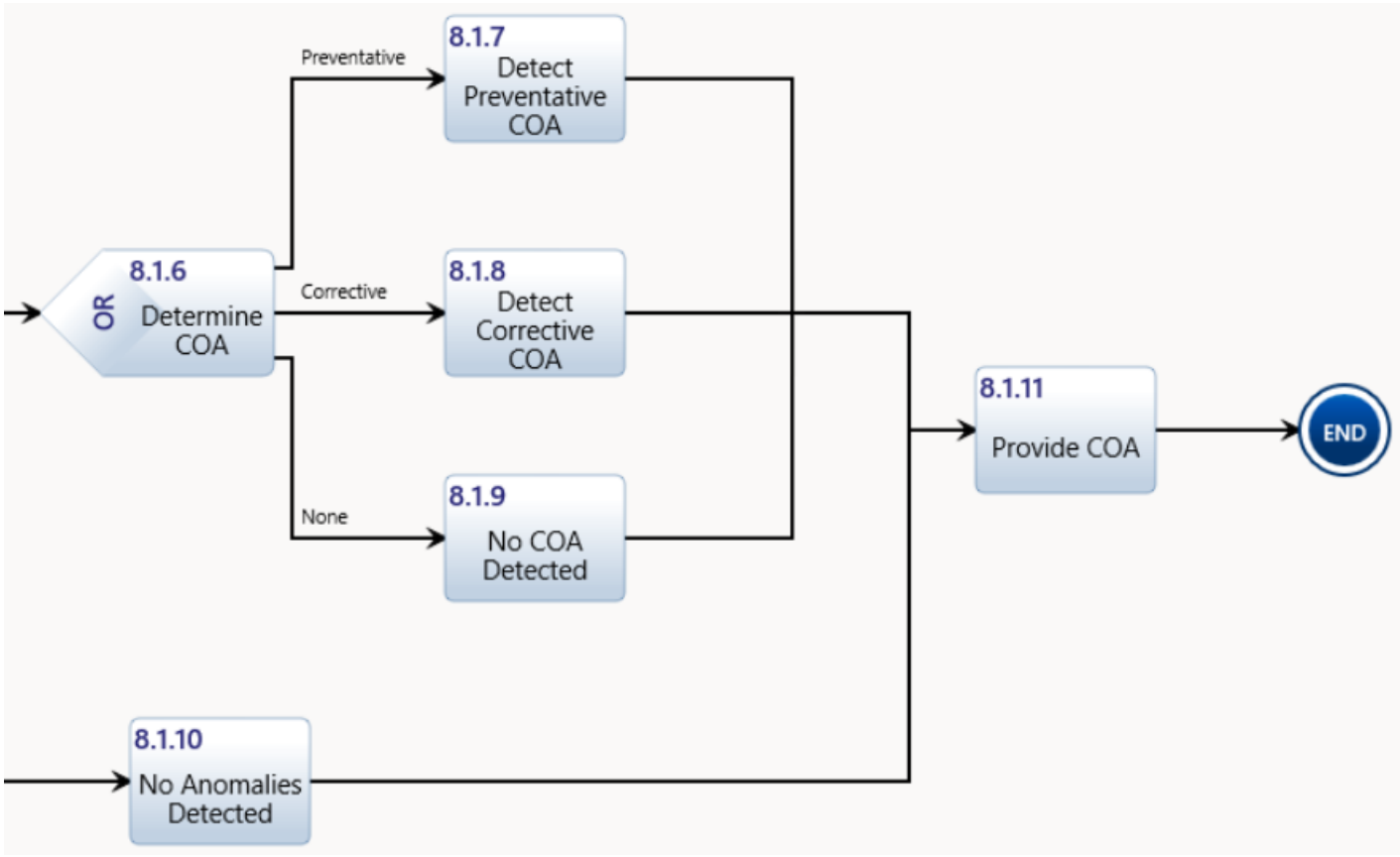


Figure 51. Condition-Based Maintenance Long-Term Action Diagram, 8.1, Part B

c. Condition-Based Maintenance Long-Term Action Diagram Description (Correct Technical Center Identification Decomposed Diagram)

As indicated in Figure 52, this sub-process starts with a decision point in the personnel side of the SWEF-Hub help desk to ascertain if the notification message identified the correct technical center, action (8.4.1). If they determine that an incorrect technical center has been identified, the SWEF-Hub personnel identify the correct technical center (8.4.2). Upon correct identification, the SWEF-Hub personnel confirm a message for delivery (8.4.3).

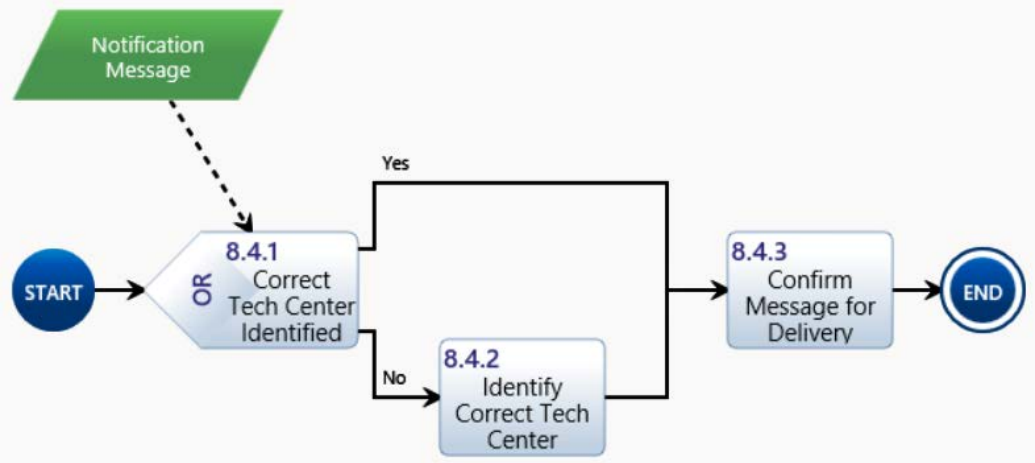


Figure 52. Condition-Based Maintenance Long-Term Action Diagram, 8.4

d. Condition-Based Maintenance Long-Term Action Diagram Description (Correct COA Identification Decomposed Diagram)

As indicated in Figure 53, this sub–process begins in the appropriate technical center where the subject matter experts check the COA provided by the ML program, action (8.7.1). After the subject matter experts complete the check, they reach a decision point (8.7.2). If they determine that it is the correct COA, then they provide the COA in action (8.7.5). If they determine that it is not the correct COA, the subject matter experts analyze the data to determine the correct COA (8.7.3). When the subject matter experts identify the correct COA (8.7.4), they provide the COA in action (8.7.5).

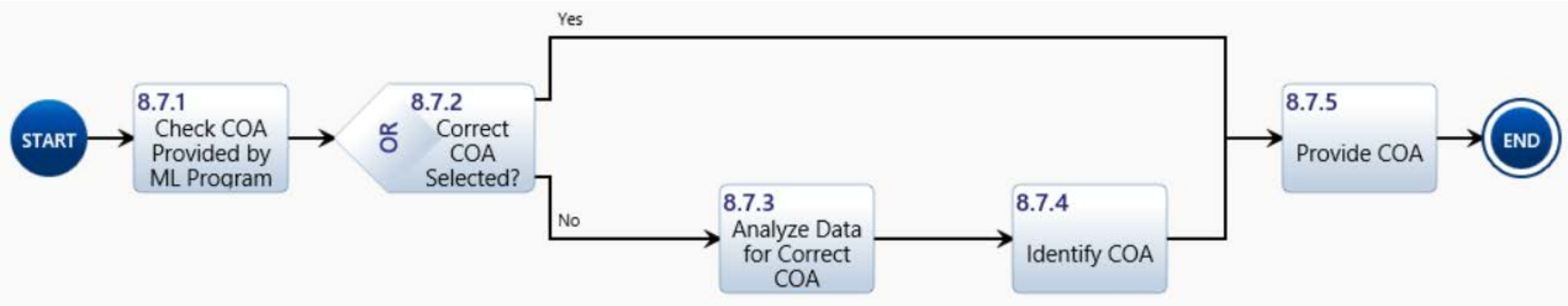


Figure 53. Condition-Based Maintenance Long-Term Action Diagram, 8.7

3. Raw Data Collection Long-Term Action Diagram Description

The raw data collection long-term action process contains two elements: ship element and the SWEF-Hub help desk. Figure 54 shows the entire process for a visual reference only, while Figures 55 and 56 show the details. The SWEF-Hub help desk has two sub-elements, the ML program and SWEF-Hub personnel. The ship element performs a maintenance action, action (2.1); action (2.1) is decomposed and described in Chapter V Section E paragraph 2.a and shown in Figure 48. The ship element secures the data using an automated process (7.2) and sends a secured email stating that the maintenance action is complete to the SWEF-Hub/ML program (7.3). The ML program receives the data (7.4), analyzes (7.5), categorizes (7.6), and stores it (7.7) using automated processes as described in the earlier scenarios of Chapter V Section E. The ML program then sends a notification email to the SWEF-Hub personnel to monitor the categorization action (9.1). The SWEF-Hub is manned 24/7, the personnel are biometrically authenticated, and its operational status is continuously monitored (1.1). When the SWEF-Hub personnel receive the notification email (9.2), they confirm the categorization (9.3); action (9.3) is shown decomposed in Chapter V Section E paragraph 3.b below and illustrated in Figure 57. The SWEF-Hub personnel send a confirmation message to the ML program (9.4). The ML program receives the confirmation message (9.5), then logs and records the decision (9.6). The ML program stores the maintenance data (7.7) in the database for future access by its automated processes.

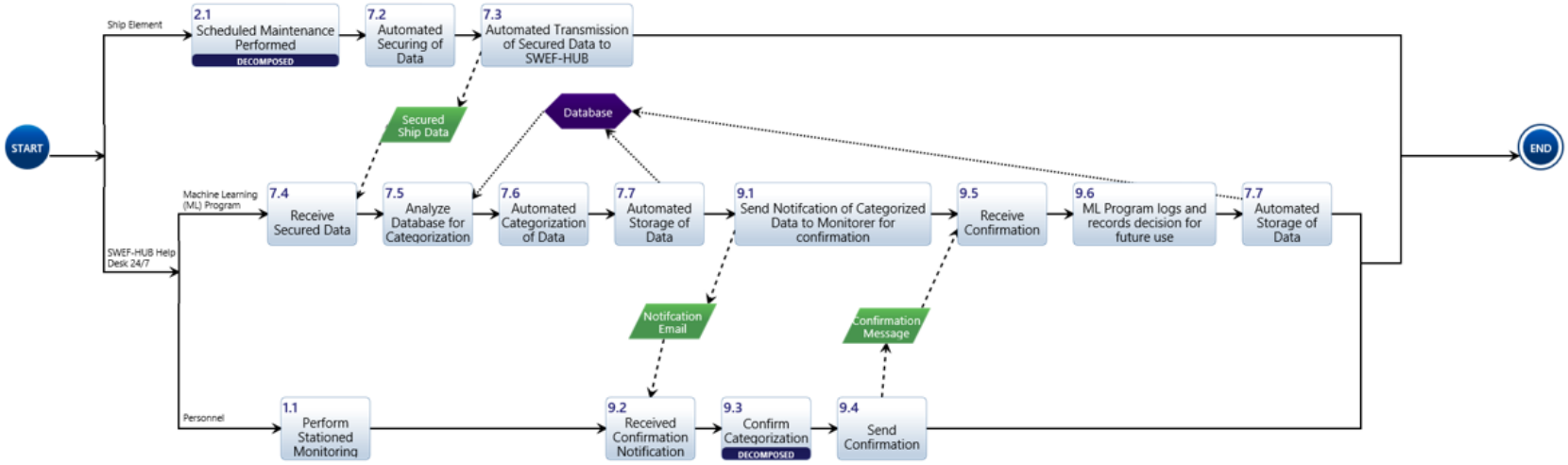


Figure 54. Raw Data Collection Long-Term Action Diagram

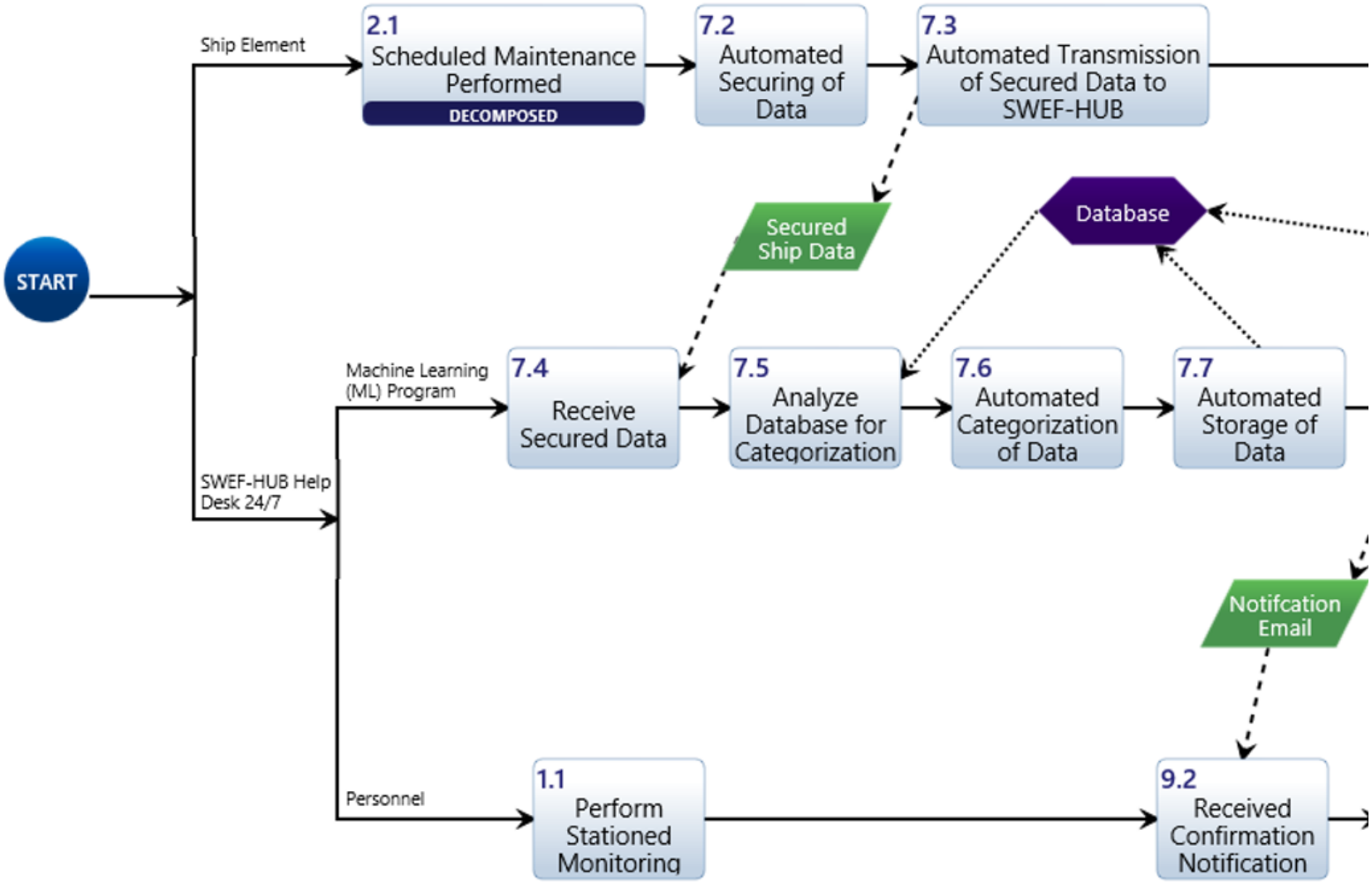


Figure 55. Raw Data Collection Long-Term Action Diagram, Part A

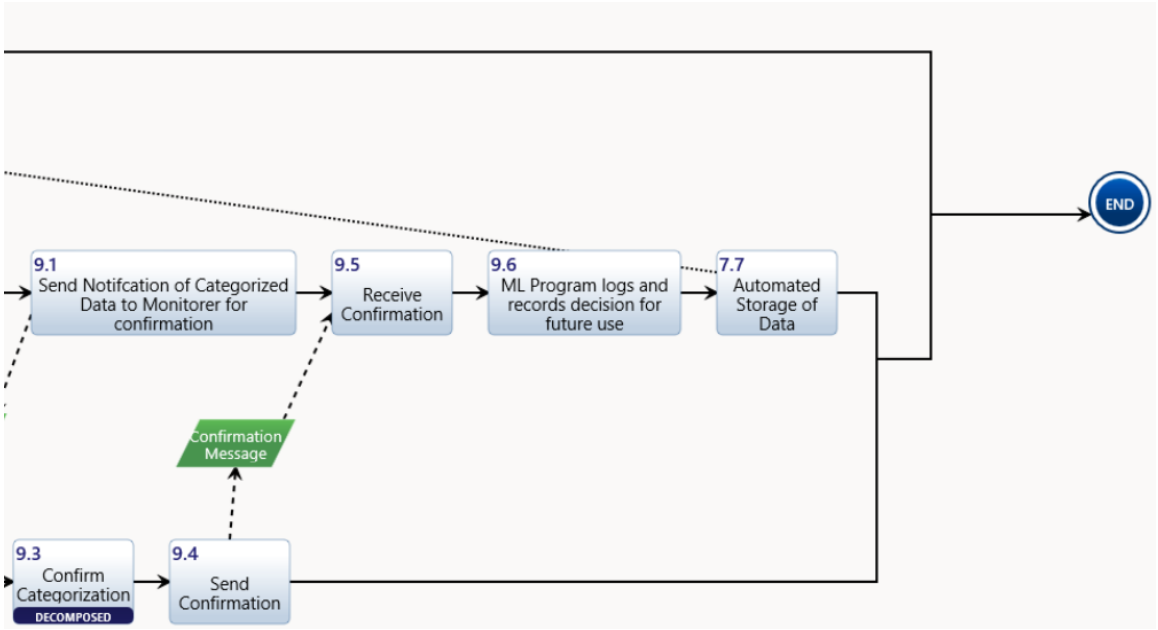


Figure 56. Raw Data Collection Long-Term Action Diagram, Part B

a. Raw Data Collection Long-Term Action Diagram Description (Scheduled Maintenance Decomposed Diagram)

The raw data collection long-term action diagram shown in Figure 54 contains a scheduled maintenance performed action (2.1). Action (2.1) is decomposed and described in Chapter V Section E paragraph 2.a and shown in Figure 48.

b. Raw Data Collection Long-Term Action Diagram Description (Data Categorization Check Decomposed Diagram)

As indicated in Figure 57, the personnel at the SWEF-Hub are responsible for this sub process. It begins with a decision point to determine whether the data has been properly categorized, action (9.3.1). If the SWEF-Hub personnel determine that the data has been incorrectly categorized, they subject the collected data to further review (9.3.2) and categorize it appropriately (9.3.3). Once the SWEF-Hub personnel determine that the data is properly categorized, they confirm the categorization (9.3.4).

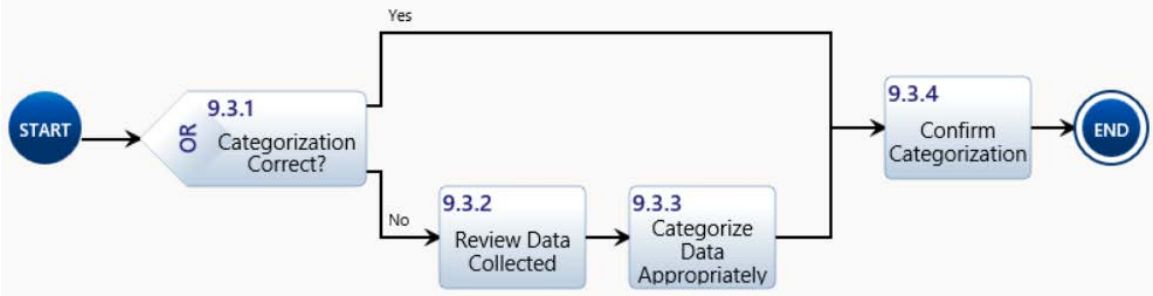


Figure 57. Raw Data Collection Long-Term Action Diagram, 9.3

4. Troubleshooting Long-Term Action Diagram Description

The troubleshooting long-term action process contains three elements: the ship, the SWEF-Hub help desk, and the technical center personnel. The complete process is shown in Figure 58 as a visual reference only, while Figures 59, 60, and 61 show the details. The troubleshooting process operates under the presumption that the data contains an anomaly. The SWEF-Hub help desk has two sub-elements, the ML program and SWEF-Hub personnel. The ship element performs automated system data enquiries, action (7.1). The ship element secures the data using an automated process (7.2) and sends a secured email stating that the maintenance action is complete to the SWEF-Hub/ML program (7.3). The SWEF-Hub is manned 24/7, the personnel are biometrically authenticated, and its operational status is continuously monitored (1.1). The ML program receives the data (7.4) and analyzes it for anomalies (10.1). When the ML program detects an anomaly (10.2), it analyses the database in order to determine the issue (10.3). If the ML system identifies an issue (10.4), it continues to analyze the database to find a solution (10.5); action (10.5) is shown decomposed in Chapter V Section E paragraph 4.b below and illustrated in Figure 63. The ML program identifies the appropriate technical center (8.2). SWEF-Hub personnel review the information to ensure that the appropriate personnel are notified (10.6); action (10.6) is shown decomposed in Chapter V Section E paragraph 4.c below and illustrated in Figure 64. SWEF-Hub personnel send a notification to the technical center. The technical center receives the notification (10.7) and access the SWEF-Hub database (10.8). The technical center reviews the solution (10.9); action (10.9) is shown decomposed in Chapter V Section E paragraph 4.d below and illustrated in Figure 65. The

technical center sends a message with COA data to the ML program of the SWEF-Hub (10.10). In turn, the SWEF-Hub sends the solution to the ship element (4.10). The ship element implements the solution (4.11). After the ship attempts to implement the solution, they reach a decision point (4.12). If the solution resolves the issue, a NOC is developed (4.14), sent to the SWEF-Hub (10.11), and stored in the database. The SWEF-Hub, using the database, identifies the appropriate technical center (2.4) and sends a closeout issue message to the technical center (10.12). The technical center receives the closeout message (10.13) and, accessing the database, reviews the NOC (4.16). The technical center accepts the NOC and closes out the issue (10.14). The technical center sends the closeout confirmation to the SWEF-Hub for closeout (2.20). An automated process stores all data (7.7). From the decision point (4.12), if the proposed solution does not resolve the issue, troubleshooting continues until the issue is resolved (4.13); action (4.13) is shown decomposed in Chapter V Section E paragraph 4.a below and illustrated in Figure 62.

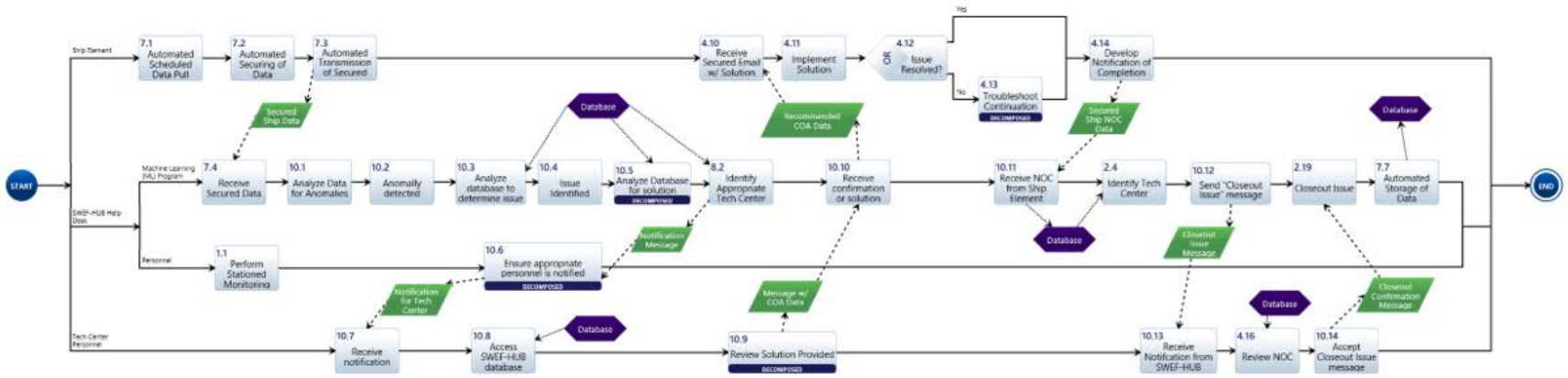


Figure 58. Troubleshooting Long-Term Action Diagram

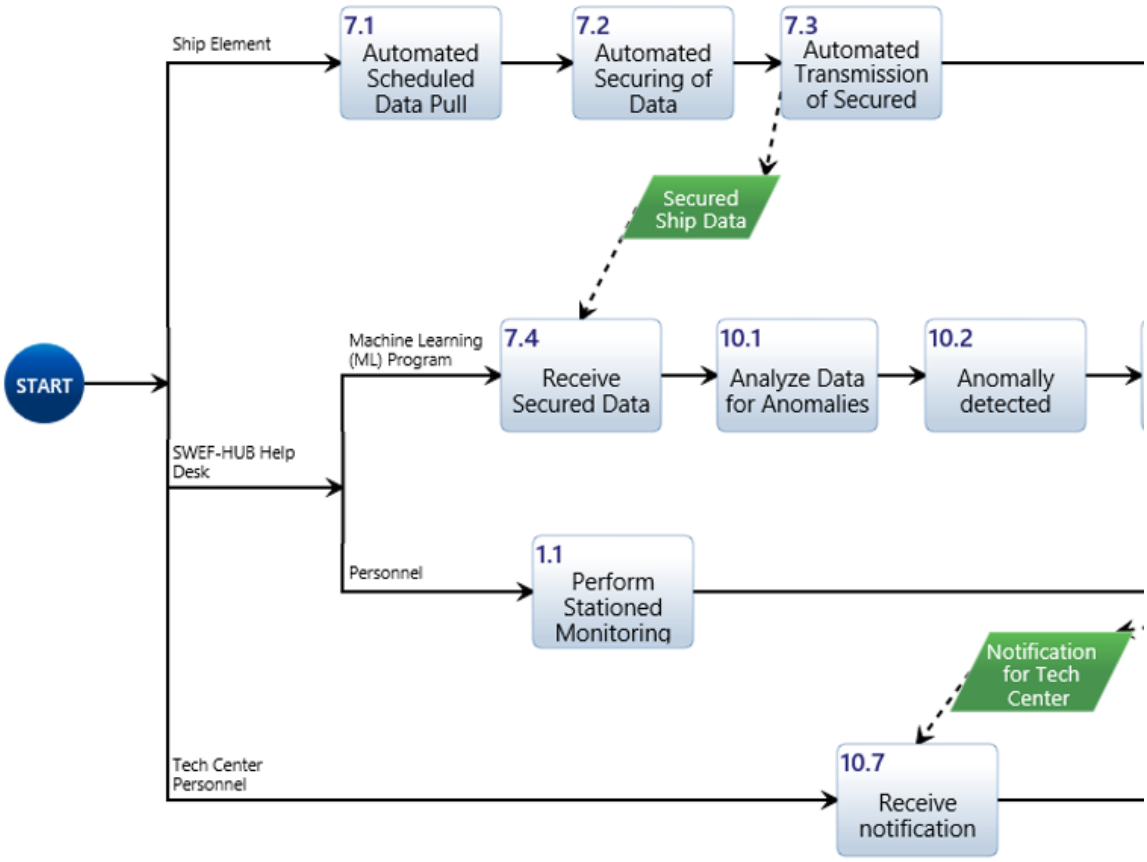


Figure 59. Troubleshooting Long-Term Action Diagram, Part A.

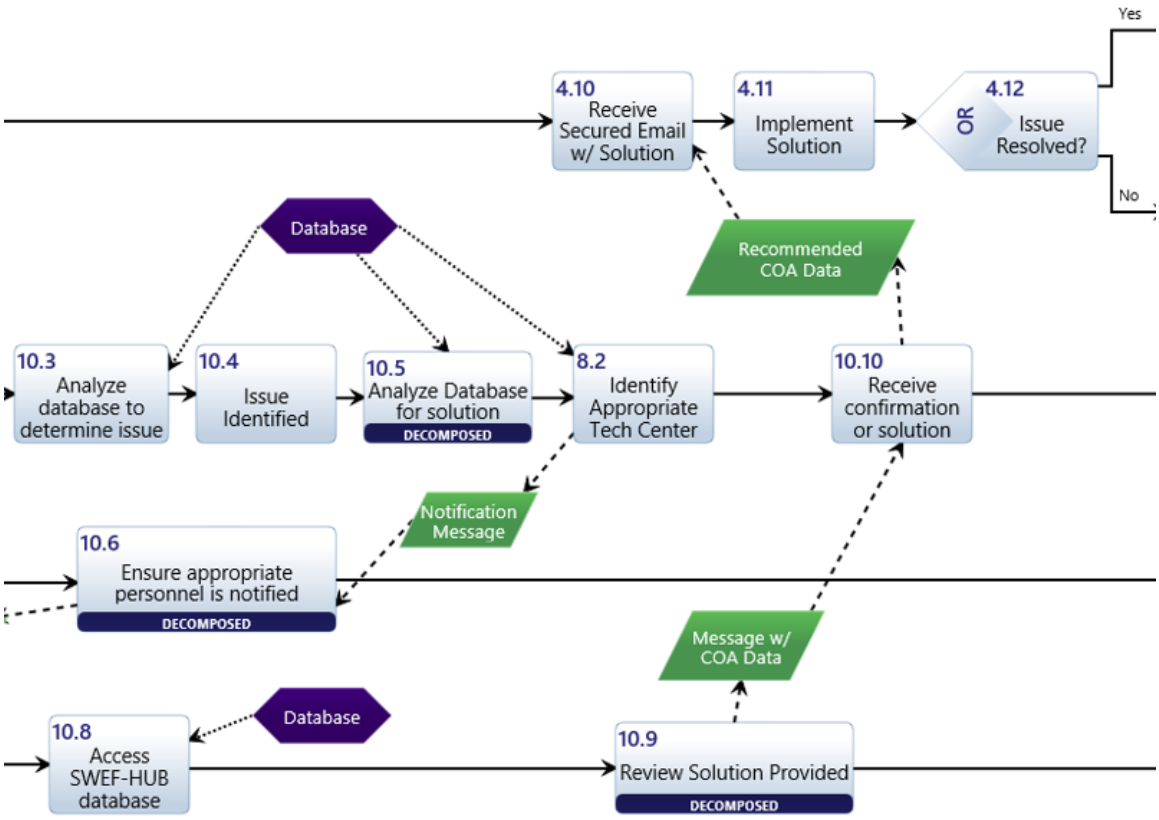


Figure 60. Troubleshooting Long-Term Action Diagram, Part B

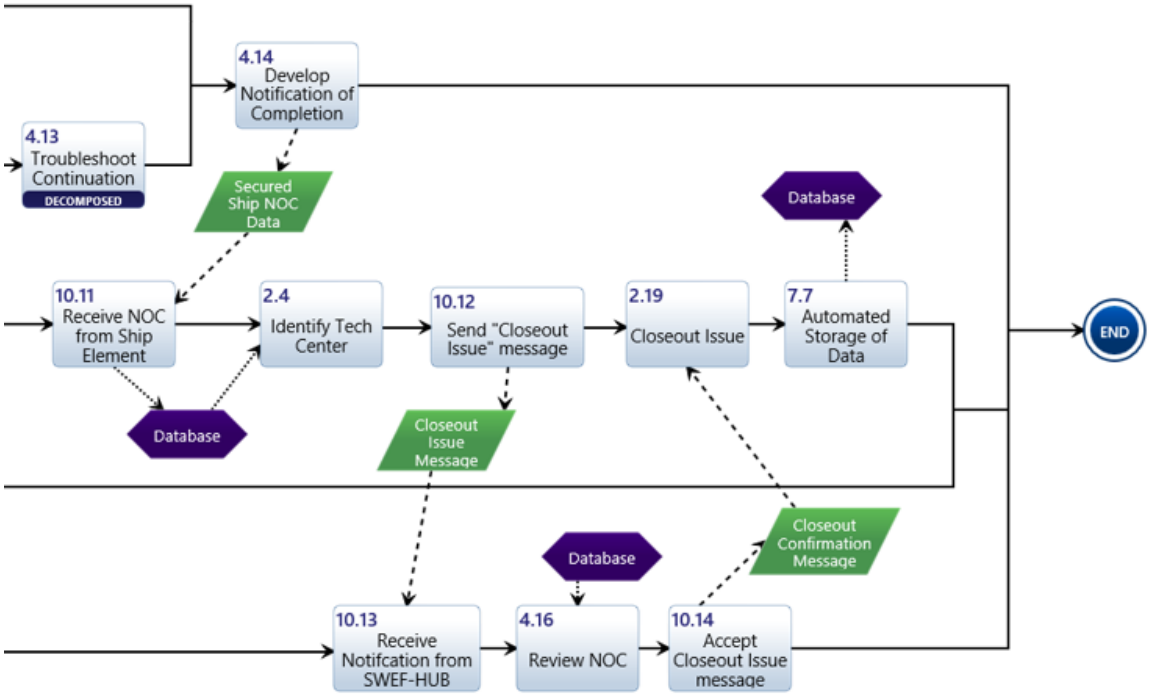


Figure 61. Troubleshooting Long-Term Action Diagram, Part C

a. Troubleshooting Long-Term Action Diagram Description (Develop Solution Decomposed Diagram)

As indicated in Figure 62, this sub-process starts in the technical center with a decision point, action (4.13.1). When the technical center resolves the issue, the sub-process ends. Otherwise the technical center continues to troubleshoot until a solution is found (4.13.2).

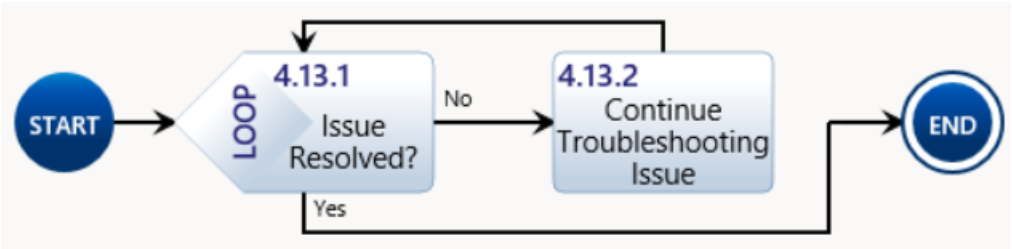


Figure 62. Troubleshooting Long-Term Action Diagram 4.13

b. Troubleshooting Long-Term Action Diagram Description (Database Analysis for Solution Decomposed Diagram)

As indicated in Figure 63, this sub-process starts with the ML program component of the SWEF-Hub help desk reviewing previous closed issues, action (10.5.1). When the ML program completes its review, it reaches a decision point (10.5.2). If the ML program finds a solution, they provide the recommended solution (10.5.3). If they do not find a solution, they develop a message (10.5.4) stating that no solution was found. The SWEF-Hub sends a notification to the appropriate personnel (10.5.5).

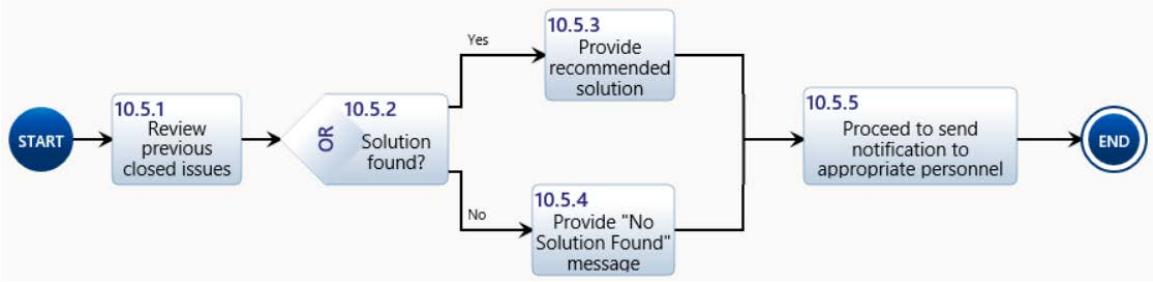


Figure 63. Troubleshooting Long-Term Action Diagram, 10.5

c. Troubleshooting Long-Term Action Diagram Description (Correct Personnel Notification Decomposed Diagram)

As indicated in Figure 64, this sub-process begins with the SWEF-Hub personnel reviewing the ML program notification message to determine whether the correct personnel have been identified for resolving the issue. This review ends in a decision point, action (10.6.1). If they determine that the correct personnel are identified, then the SWEF-Hub personnel send a notification to the correct technical center (10.6.4). If they determine that the correct personnel are not identified on the notification message, the SWEF-Hub personnel review the anomaly and issue provided by the ML program (10.6.2). The SWEF-Hub personnel identify the appropriate personnel (10.6.3) and send a notification to the correct technical center (10.6.4).

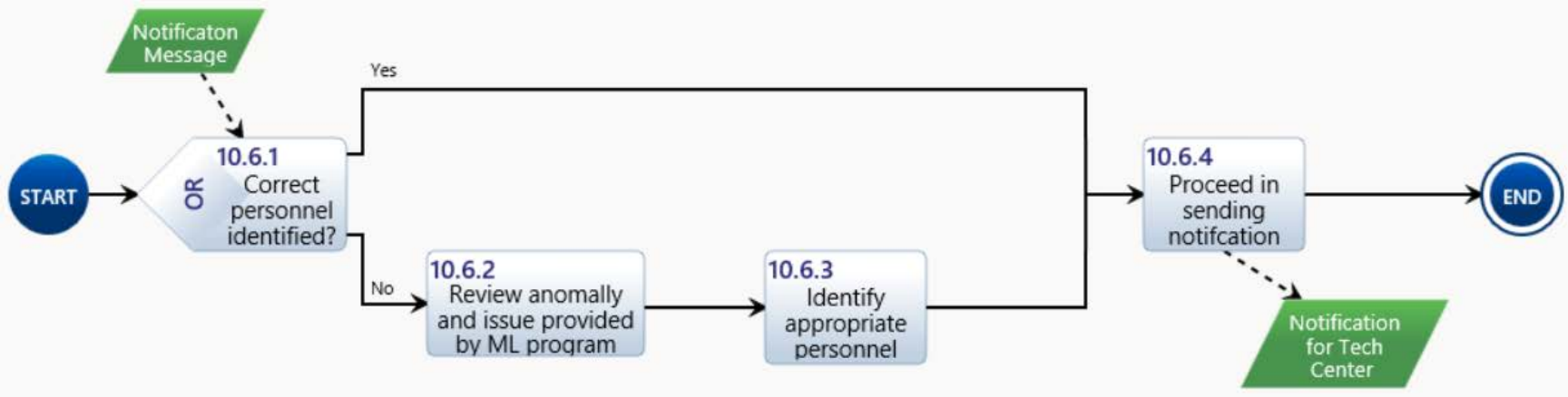


Figure 64. Troubleshooting Long-Term Action Diagram, 10.6

d. Troubleshooting Long-Term Action Diagram Description (Solution Provided Review Decomposed Diagram)

As indicated in Figure 65, this sub-process begins with the technical center personnel reviewing the message provided by the ML program through the SWEF-Hub personnel. This review ends with a decision point, action (10.9.1). If the message provided by the ML program recommends a solution and the technical center determines that it is applicable to resolving the problem (10.9.2), then the technical center personnel send the solution to the SWEF-Hub (10.9.3). Action (10.9.2) is shown decomposed in Chapter V Section E paragraph 4.d.(1) below and illustrated in Figure 66. If the technical center personnel determine that a solution has not been found, then they develop a solution (4.8); action (4.8) is shown decomposed in Chapter V Section E paragraph 4.d.(2) below and illustrated in Figure 69. When they determine a solution, the technical center personnel send the solution to the SWEF-Hub (10.9.3).

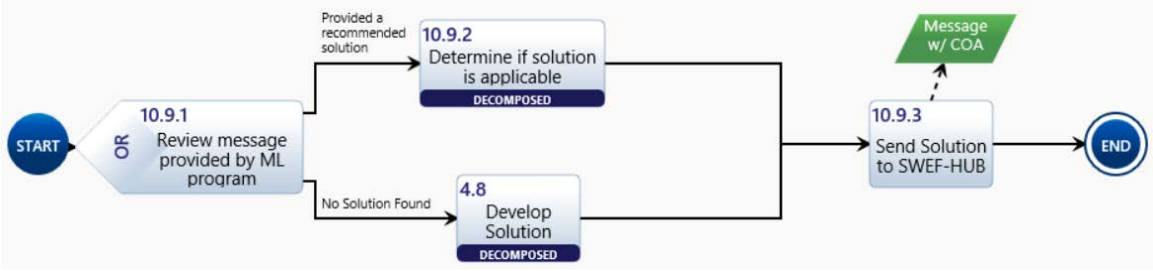


Figure 65. Troubleshooting Long-Term Action Diagram, 10.9

(1) Troubleshooting Long-Term Action Diagram Description (Solution Viable Decomposed Diagram)

Figure 66 shows the entire process as a visual reference only, while Figures 67 and 68 show the details. This sub-process begins with the technical center personnel reviewing the ML program message to determine whether the solution COA is viable and applicable. This review ends at a decision point, action (10.9.2.1). If they determine that a solution is viable, the technical center provides the applicable solution (10.9.2.10) and completes the sub-process. If the technical center determines that the solution is not viable, they indicate that the solution is incorrect (10.9.2.2) and troubleshoot the issue (10.9.2.3). After

troubleshooting the issue, the technical center reaches another decision point (10.9.2.4). If the technical center developed a viable solution, they provide the applicable solution (10.9.2.10) and complete the sub-process. If the technical center has not yet developed a solution, they reach another decision point (10.9.2.5). If the technical center subject matter experts determine that a solution can be developed remotely, they continue troubleshooting (10.9.2.6). After continuing troubleshooting, the technical center reaches another decision point (10.9.2.7). If the technical center has resolved the issue, they provide the applicable solution (10.9.2.10) and complete the sub-process. If they have not resolved the issue, they continue troubleshooting (10.8.2.8) until the issue is resolved, then provide the applicable solution (10.9.2.10) and complete the sub-process. If the solution cannot be developed remotely per decision point (10.9.2.5), then the technical center sends personnel to the ship to troubleshoot (10.9.2.9) and provides this as the solution (10.9.2.10), completing the sub-process.

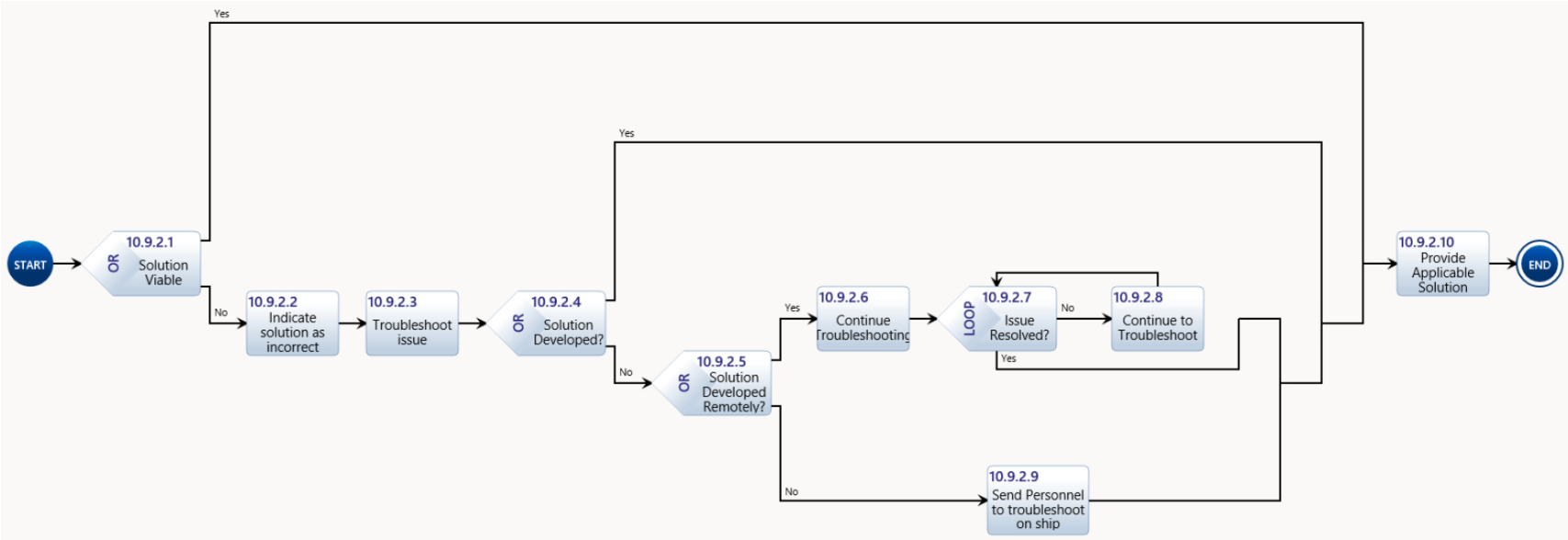


Figure 66. Troubleshooting Long-Term Action Diagram, 10.9.2

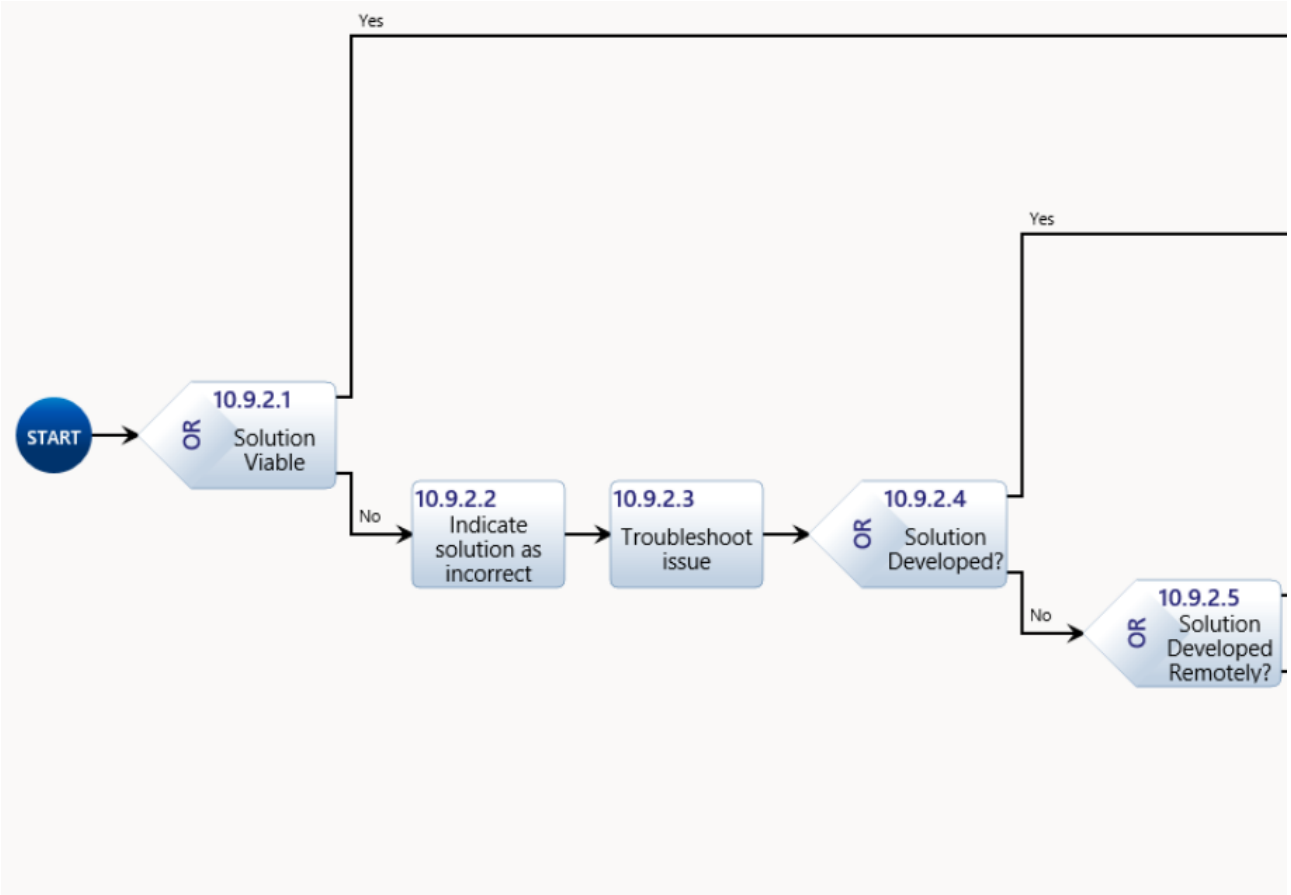


Figure 67. Troubleshooting Long-Term Action Diagram, 10.9.2, Part A

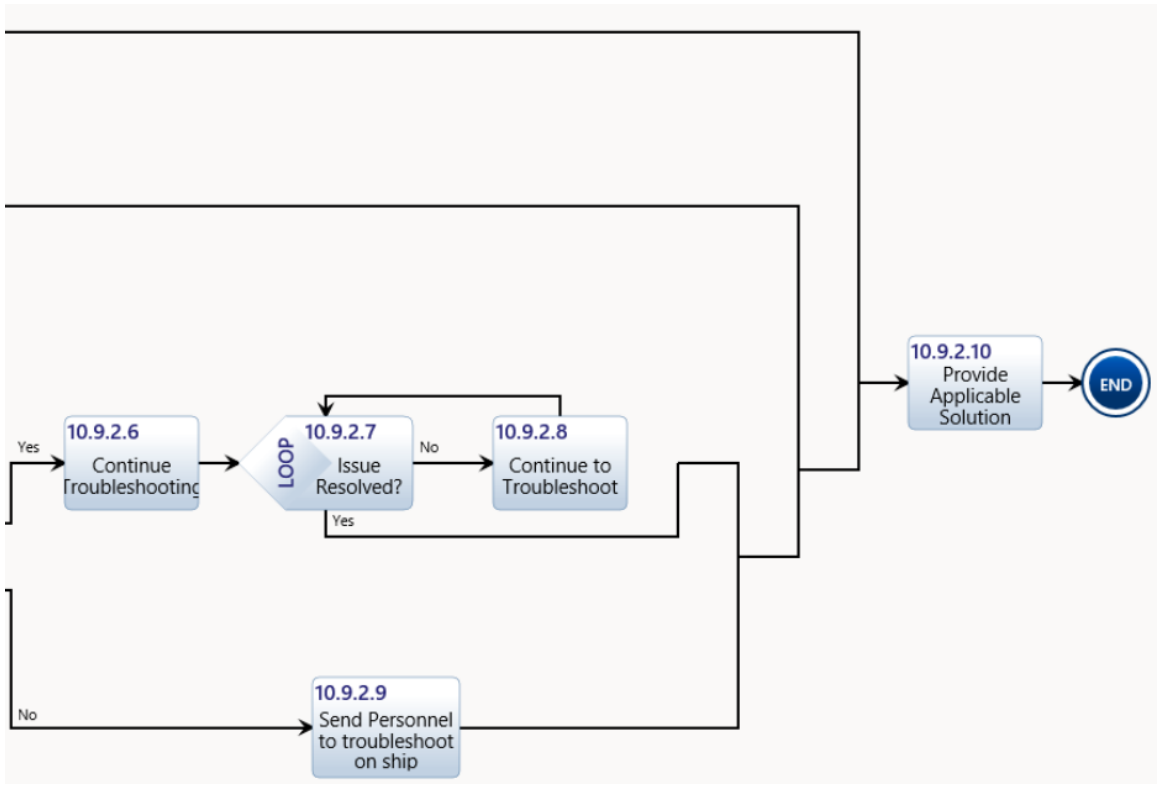


Figure 68. Troubleshooting Long-Term Action Diagram, 10.9.2, Part B

(2) Troubleshooting Long-Term Action Diagram Description (Troubleshoot/ Solution Decomposed Diagram)

As indicated in Figure 69, this sub-process starts in the technical center by reviewing past data for a solution to a similar issue, action (4.8.1). After reviewing past data, the technical center reaches a decision point (4.8.2). If the technical center finds a solution (4.8.8), they send the solution to the SWEF-Hub (4.8.9). If the technical center does not find a solution, they reach another decision point (4.8.3). If the technical center decides that they cannot develop a solution remotely, they send technical personnel to troubleshoot and resolve the issue (4.8.4) and send a message to the SWEF-Hub stating the solution (4.8.9). If the technical center determines that a solution can be developed remotely, troubleshooting begins at the technical center (4.8.5) and triggers another decision point (4.8.6). If the technical center has not yet developed a solution, they continue troubleshooting (4.8.7) until the issue is resolved, then send the solution to the SWEF-Hub (4.8.9).

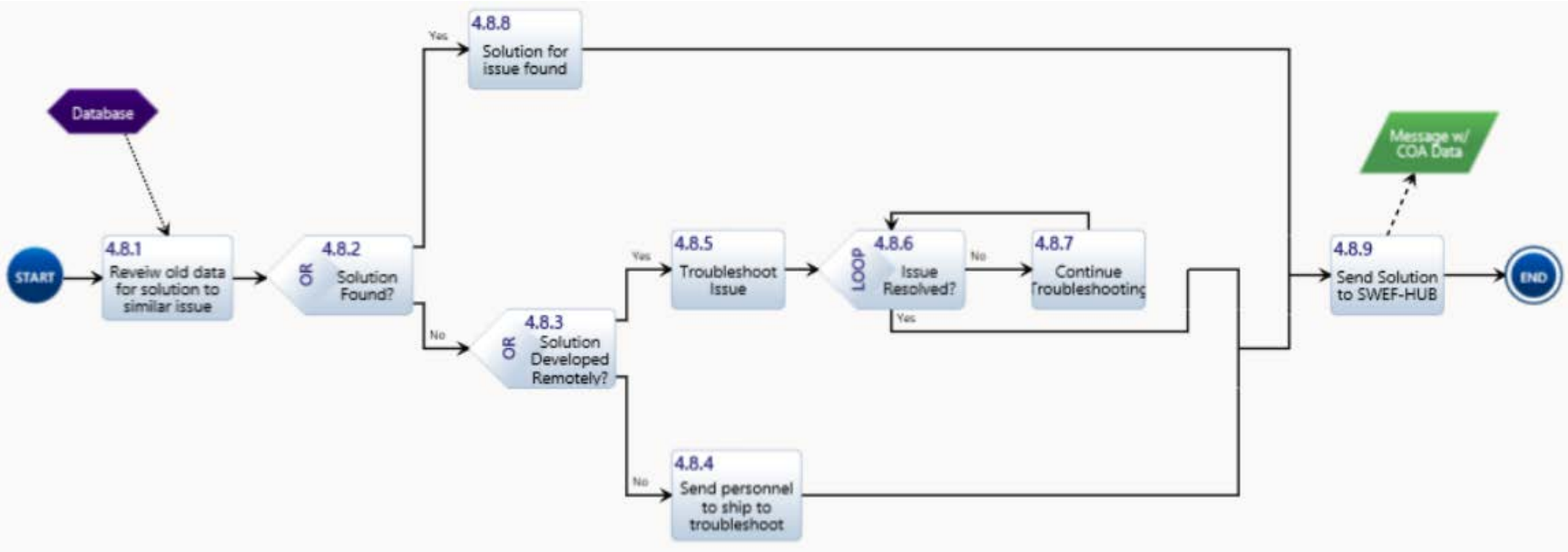


Figure 69. Troubleshooting Long-Term Action Diagram, 4.8

5. Software Upgrade Long-Term Action Diagram (and Correct Technical Center Identification Decomposed Diagram) Description

The software upgrade long-term action process contains three elements: the ship element, the SWEF-Hub, and the technical center. Figure 70 shows the complete process as a visual reference only, while Figures 71 and 72 show the details. The SWEF-Hub has two sub-components: the ML program and SWEF-Hub personnel. The technical center develops a software upgrade or patch, action (5.1), and securely sends it to the ML program/SWEF-Hub (5.2). The ML program receives the software upgrade or patch (5.3) and stores the software data in the database. The ML program accesses the database and analyses the software upgrade or patch for distribution to the appropriate ship element (5.4). When the ML program, using the database, identifies the ship element (5.5), the ML program/SWEF-Hub sends out the software upgrade or patch. The ship element receives (5.6) and implements the software upgrade or patch (5.7). Upon completion of the action, the ship element sends the NOC data to the ML program/SWEF-Hub (5.8). The ML program/SWEF-Hub receives the NOC data (11.1) and stores the software upgrade or patch NOC using an automated process (7.7) in the database. The ML program using the database, identifies the appropriate technical center (2.4) and forwards the NOC to the SWEF-Hub personnel. The SWEF-Hub personnel receive the NOC (2.3), confirm that it is properly stored and that the correct technical center has been chosen (11.2); action (11.2) is shown decomposed in Chapter V Section E paragraph 5.a below and illustrated in Figure 73. The SWEF-Hub personnel send the software upgrade or patch related NOC to the technical center and a confirmation message to the ML program. The technical center receives the NOC for the software upgrade or patch (11.3). The ML program receives the confirmation message (11.4) and stores the NOC data in the database using automated processes (7.7). The SWEF-Hub is manned 24/7, the personnel are biometrically authenticated, and its operational status is continuously monitored (1.1).

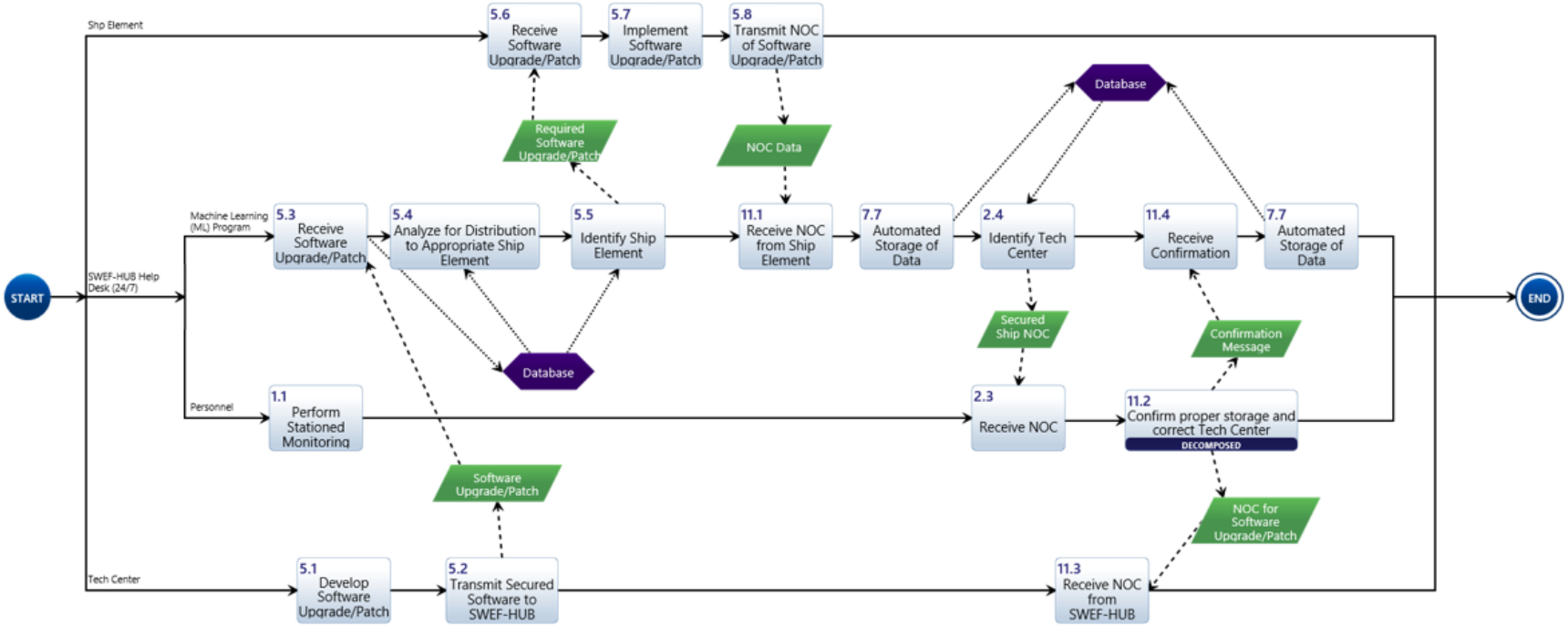


Figure 70. Software Upgrade Long-Term Action Diagram

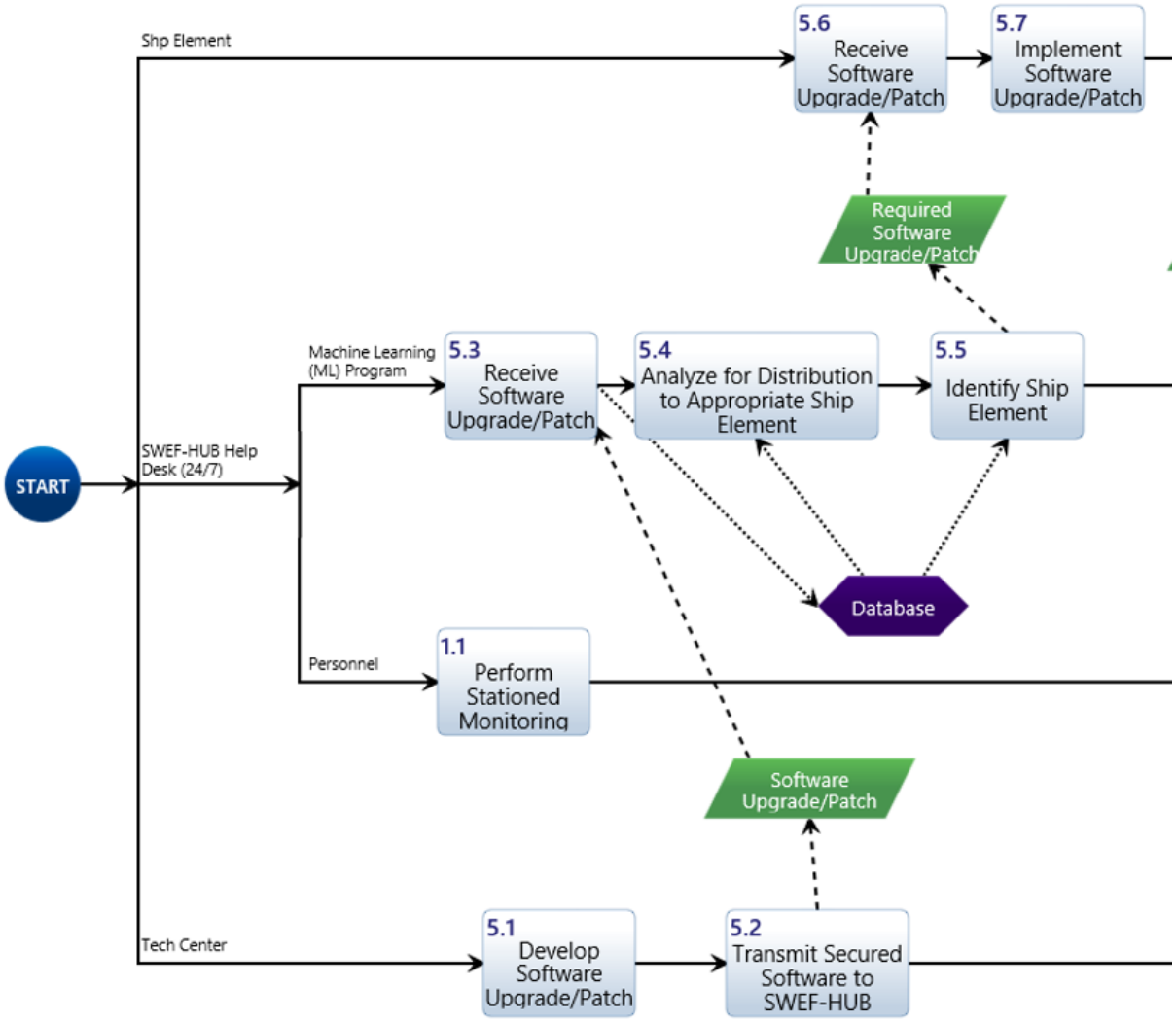


Figure 71. Software Upgrade Long-Term Action Diagram, Part A

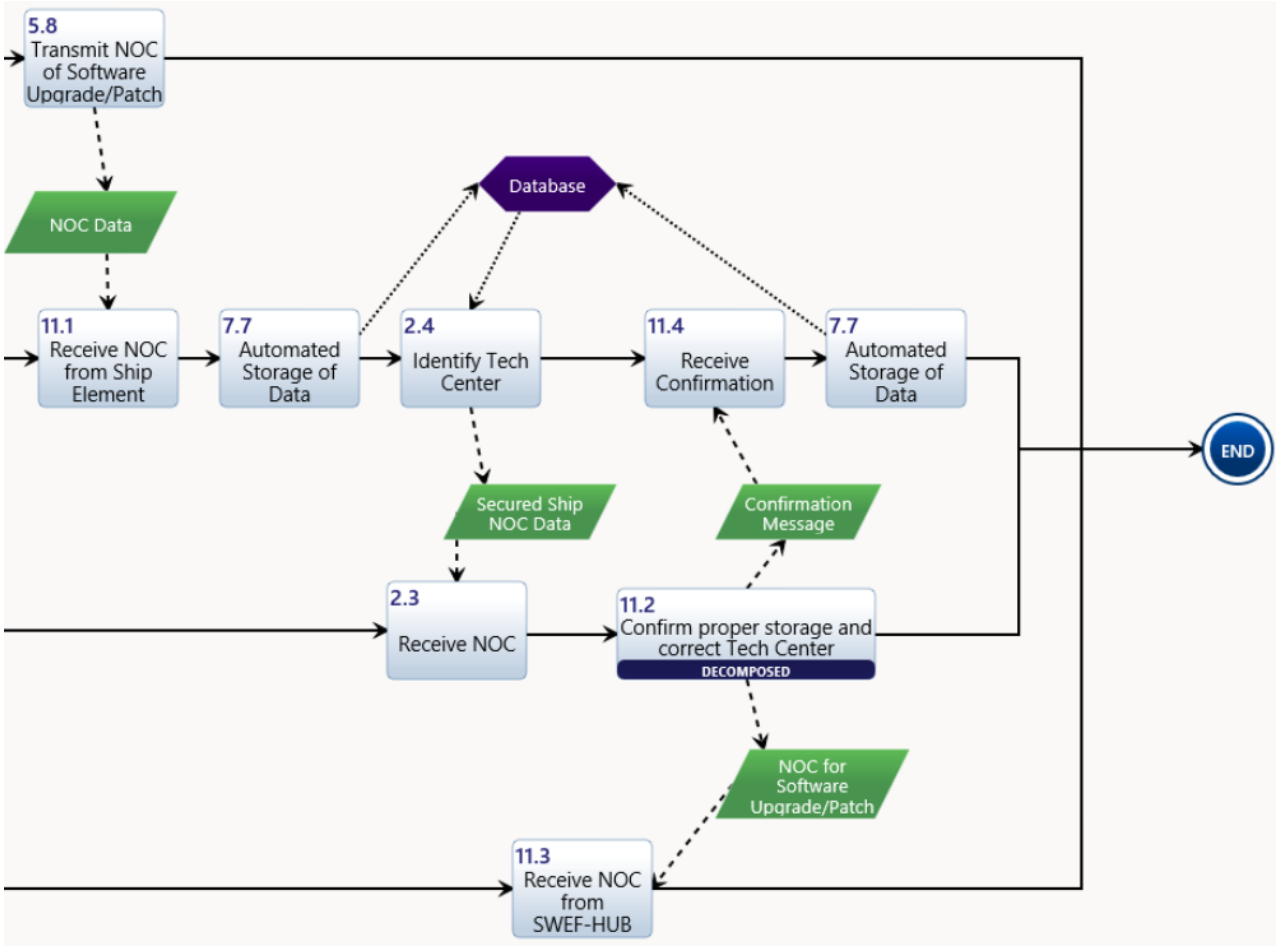


Figure 72. Software Upgrade Long-Term Action Diagram, Part B

The Software upgrade long-term action diagram (Correct technical center identification decomposed diagram) is described next. As indicated in Figure 73, this sub-process starts with a SWEF-Hub personnel review of the secured ship NOC data. The review ends in a decision point (11.2.1). If the SWEF-Hub personnel determine that the correct technical center was identified, they proceed in sending notifications to the technical center and ML program (11.2.4). If the SWEF-Hub personnel determine that the correct technical center is not properly identified, they determine the correct categorization (11.2.2) and identify the correct technical center (11.2.3). When they have correctly identified the technical center, they send a notification to the technical center and ML program (11.2.4).

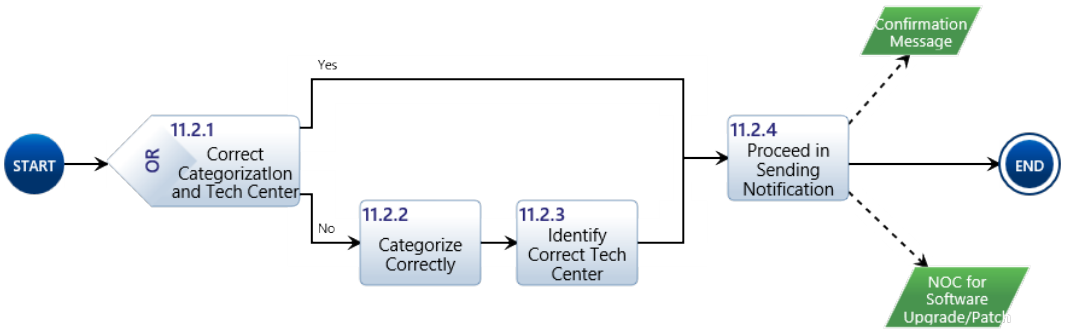


Figure 73. Software Upgrade Long-Term Action Diagram, 11.2

6. Secondary Collaboration Long-Term Action Diagram Description

The secondary collaboration long-term action process contains three elements: the system element, the SWEF-Hub help desk, and the technical center personnel. The SWEF-Hub element is composed of two sub-elements: the ML program and personnel. Figure 74 shows the entire process for visual reference only, while Figures 75, 76, 77, and 78 show the details.

The system element sends a secure email request to the SWEF-Hub help desk/ML program, action (6.1). The SWEF-Hub is manned 24/7, the personnel are biometrically

authenticated, and its operational status is continuously monitored (1.1). The ML program receives the request (6.2), accesses the database to process the request (12.1), accesses the database to identify the appropriate technical center (12.2), and transmits the message to the helpdesk personnel for confirmation (12.3). Once the SWEF-Hub help desk personnel receives the data (12.4), they analyze it (12.5), then confirm and forward the request to the appropriate technical center (12.6). Action (12.5) is shown decomposed in Chapter V Section E paragraph 6.a below and illustrated in Figure 79. The technical center receives the request (6.6), approves it (6.7), and sends the approval to the SWEF-Hub ML program (6.8). Once received by the SWEF-Hub ML program (6.9), the ML program accesses a system element database (12.7) to identify the system element (12.8) and sends an approval message to the system element (12.9). Once the system element receives the approval message (6.11) it transmits the data needed for the simulated testing to the SWEF-Hub (6.12). Technical center personnel go to the SWEF-Hub to setup the system (6.13) and prepare the SWEF-Hub for the simulated test environment (6.14); action (6.14) is shown decomposed in Chapter V Section E paragraph 6.b below and illustrated in Figure 80. The ML program is implemented to test the system (12.10). It assimilates the test system (12.11), the ML program receives the data from the system element (6.15), implements the data into the system (12.12). The ML program transmits a message to begin the test (12.13). Once the technical center receives the message (12.14), it sends a confirmation to begin the test (12.15). The ML program receives the confirmation (12.16), runs the simulation (6.17), and records the test results (6.18). An automated process stores the data (7.7). The technical center reviews the test results (12.17), then sends a command to forward the test results (12.18). The ML program receives the command to forward the test results (12.19) and forwards the test results to the system element (12.20). The system element receives the results (6.20). Data is stored throughout the process.

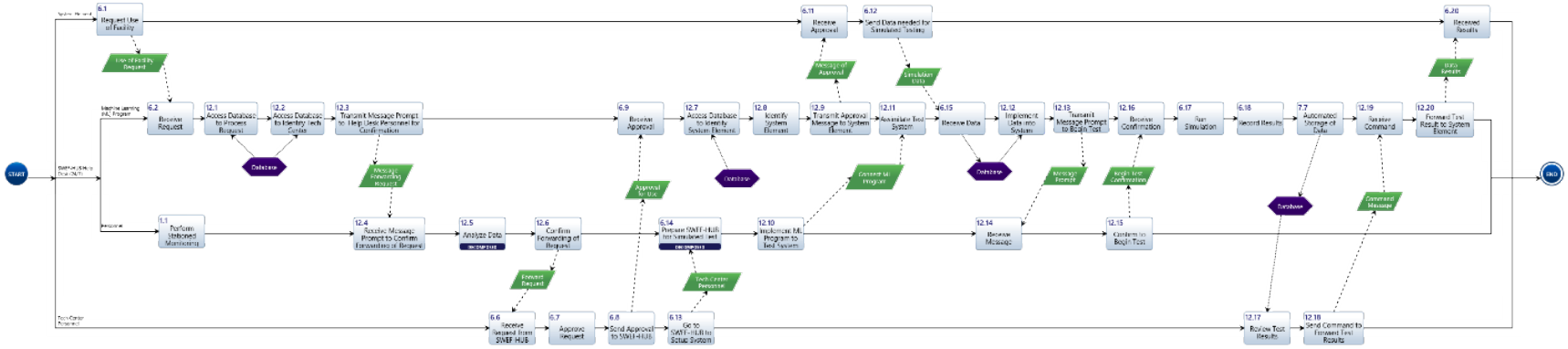


Figure 74. Secondary Collaboration Long-Term Action Diagram

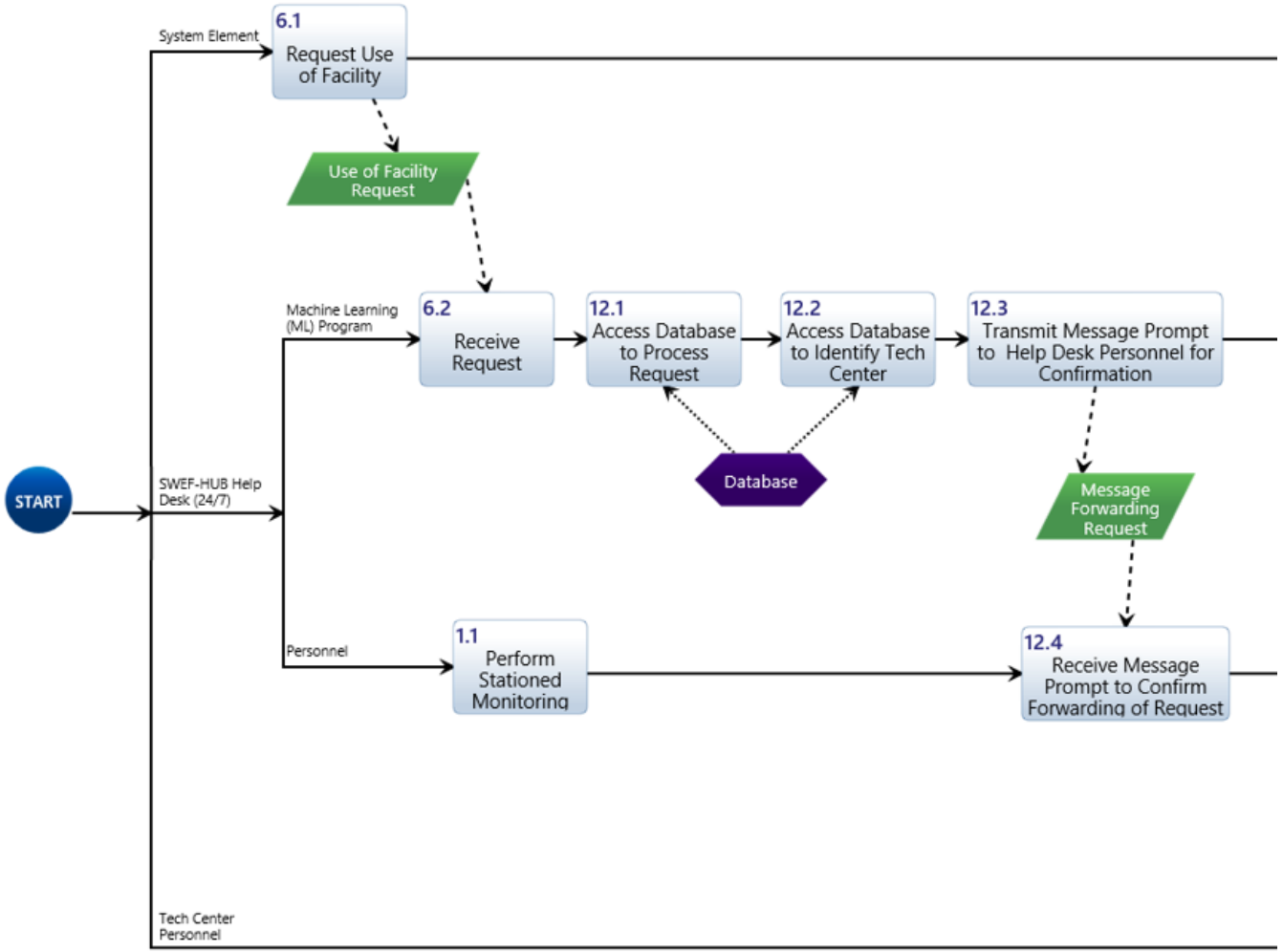


Figure 75. Secondary Collaboration Long-Term Action Diagram, Part A

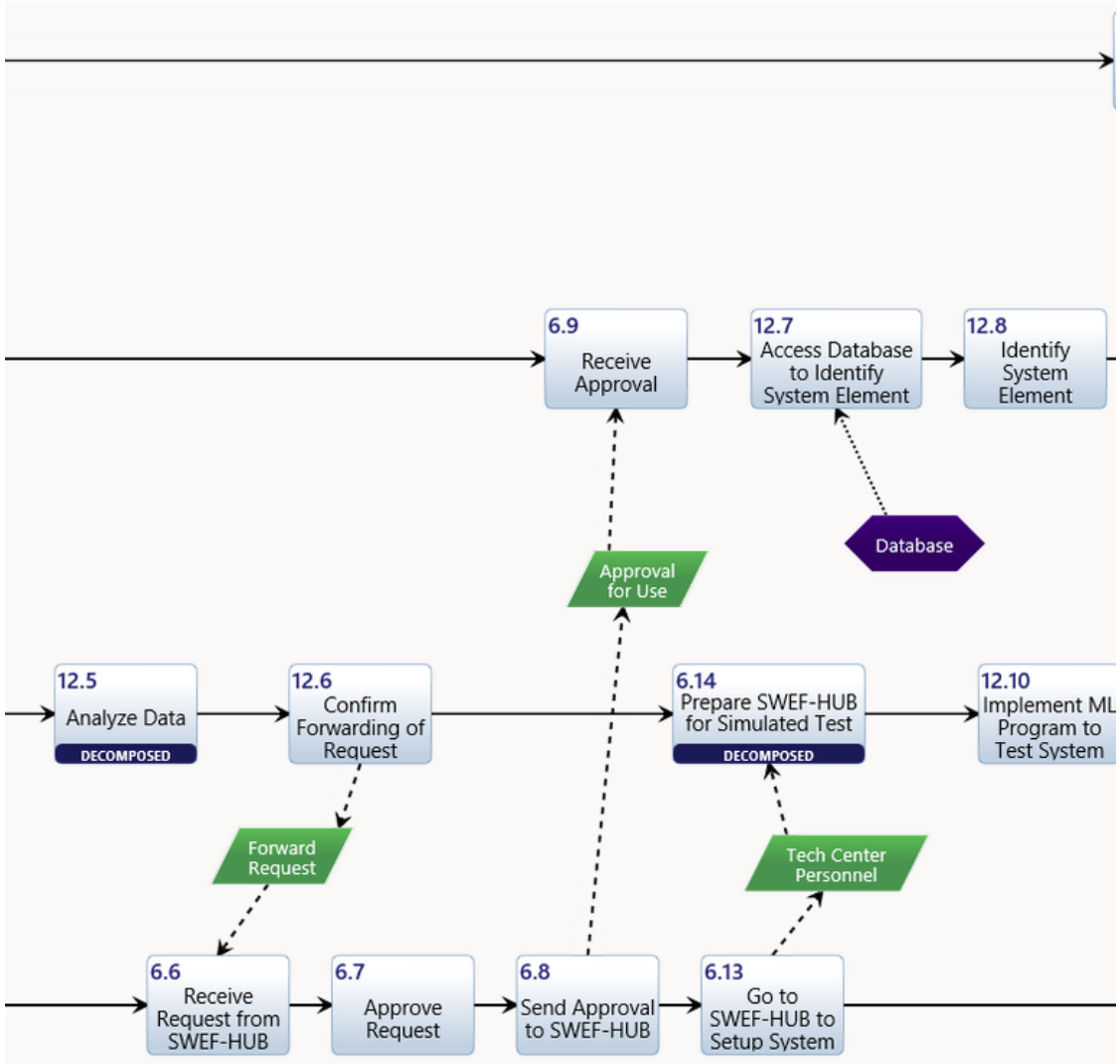


Figure 76. Secondary Collaboration Long-Term Action Diagram, Part B

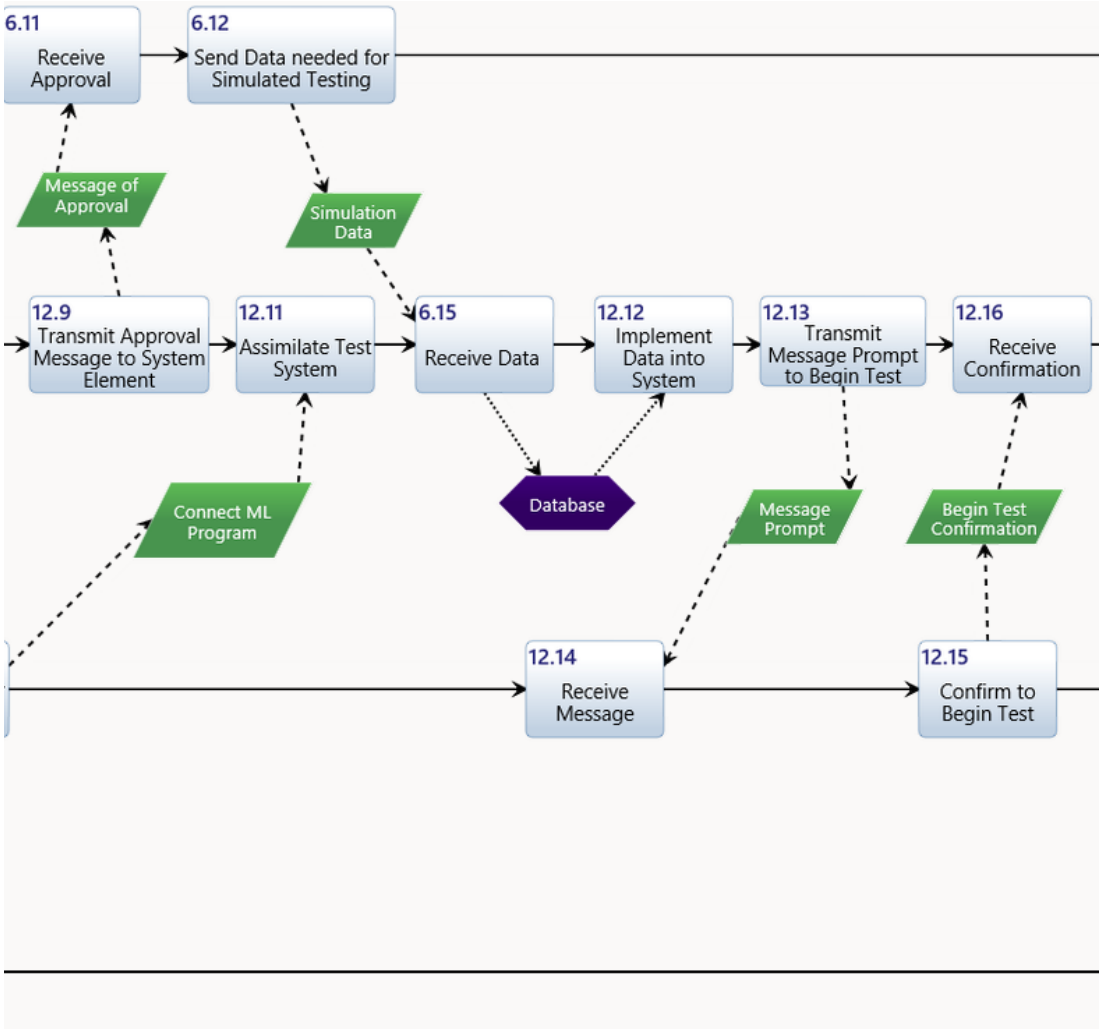


Figure 77. Secondary Collaboration Long-Term Action Diagram, Part C

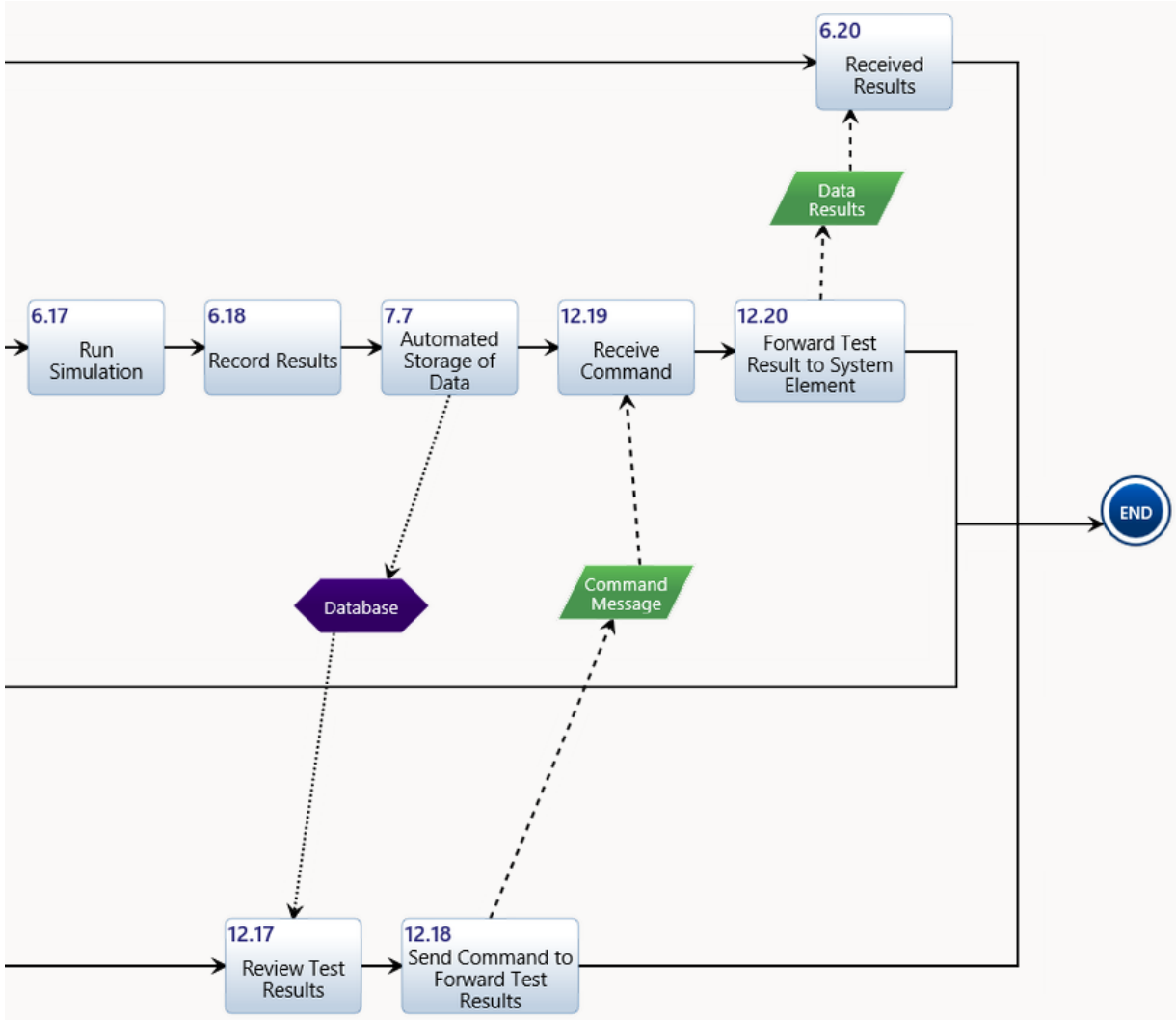


Figure 78. Secondary Collaboration Long-Term Action Diagram, Part D

a. Secondary Collaboration Long-Term Action Diagram Description (Correct Technical Center Identification Decomposed Diagram)

As indicated in Figure 79, this sub-process starts with a decision point in the personnel side of the SWEF-Hub help desk. The personnel determine whether the correct technical center was identified, action (12.5.1). If they determine that the correct technical center is not properly identified, they identify the correct technical center (12.5.2). Once they identify the correct technical center, a notification is sent (12.5.3).

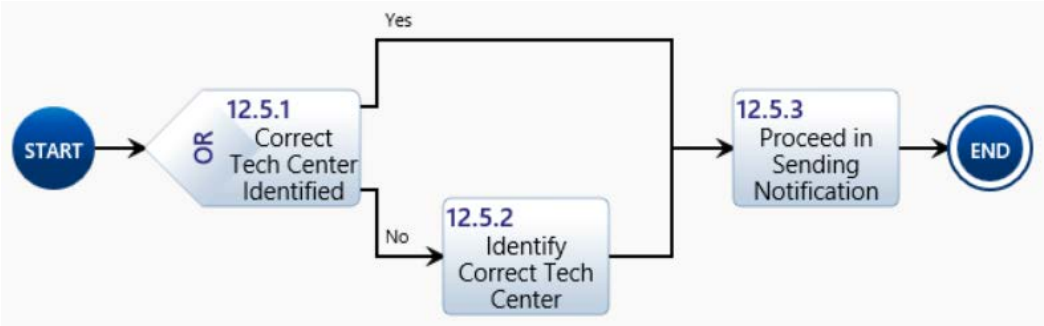


Figure 79. Secondary Collaboration Long-Term Action Diagram, 12.5

b. Secondary Collaboration Long-Term Action Diagram Description (Determination of Requirements for Testing Decomposed Diagram)

As indicated in Figure 80, this sub-process starts at the SWEF-Hub help desk by determining the hardware requirements for testing, action (6.14.1). After establishing the hardware requirements, they determine the software requirements (6.14.2). Then they determine the system layout (6.14.3) and setup the required system (6.14.4).

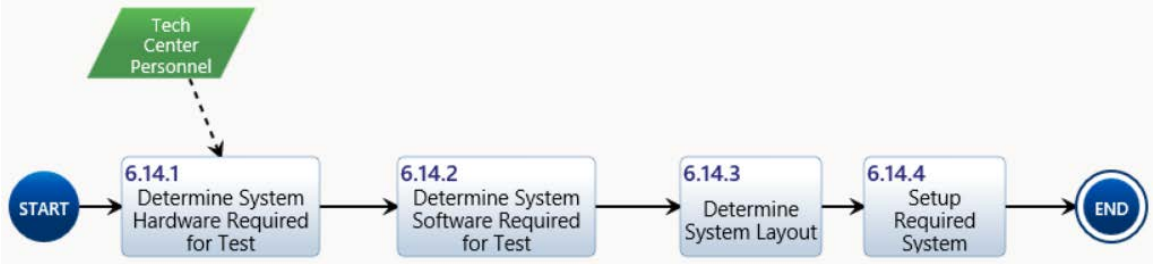


Figure 80. Secondary Collaboration Long-Term Action Diagram, 6.14

F. FUNCTIONAL TO PHYSICAL AND PHYSICAL ARCHITECTURES

As part of the process to create the Physical Architecture (PA), it is necessary to have a diagram that illustrates the transition of architectures from functional to physical. After this diagram is created, the derived physical elements are utilized in the development of the physical architecture. Other elements are added in the process and these added elements, though not mentioned in the functional architecture, become part of physical architecture because they are essential for the proper functioning of the SWEF-Hub. For example, in the physical architecture, the biometric security system and HVAC (cooling system) are part of continuous functions performed to protect computer systems in the SWEF-Hub. The biometrics computer system provides alerts to the users when hackers are trying to penetrate the system and the cooling system keeps the room at the proper temperature; both actions are occurring at all times. Similar to the biometric security system and HVAC, the power generator is not considered in the functional to physical architecture as it is a backup unit for power blackouts only; for this reason, it is only considered in the physical architecture. Other sub-elements are created to further define the physical architecture. This leads to the creation of the near-term and long-term physical architectures.

1. Functional to Physical Architecture Diagram Description

The functional to physical architecture diagram, Figure 81, shows the different functions previously derived from requirements. These functions are in black rectangles and use the original numbering. These functions are then used to derive the first set of physical elements for the physical architecture. The physical elements are in blue rectangles and numbered using the prefix PA (physical architecture) prior to the number. This numbering format is temporary; a new numbering is used in the physical architectures. As it is shown in the figure, several physical elements perform various functions, and in some cases, several physical elements perform only one function.

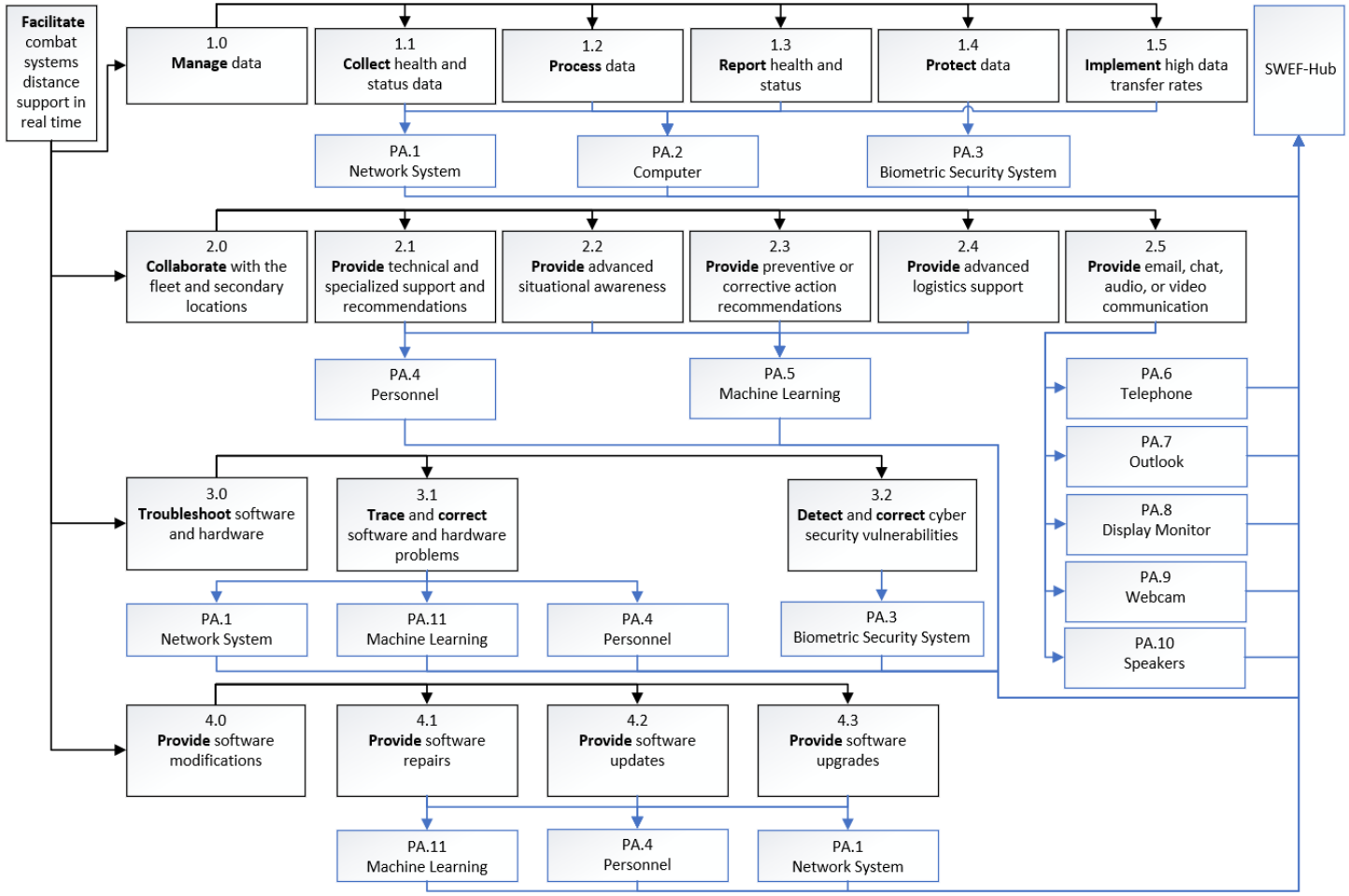


Figure 81. Functional to Physical Architecture Diagram

2. Physical Hierarchy Near-Term Diagram Description

Level zero of the physical architectures consists of the SWEF-Hub. Level one of the physical architecture consists of communication (network system), help desk, power generator, HVAC system, and the biometric security system. Level two beneath communications consists of the communication devices: antenna, router, transmitter, and receiver. Level two beneath the help desk consists of the components to reach the help desk: telephone, personnel, and computer. Level three beneath computer consists of the software and hardware. Level four beneath software consists of: the operating system, Microsoft Outlook, database management tools, and combat system software. Level four beneath hardware consists of the physical components including: the display monitor, motherboard, and power supply. Level five beneath the motherboard consists of physical components including: the processor, the graphics card, the network identification card, a solid-state drive, and the random-access memory (RAM). See Figure 82 for details.

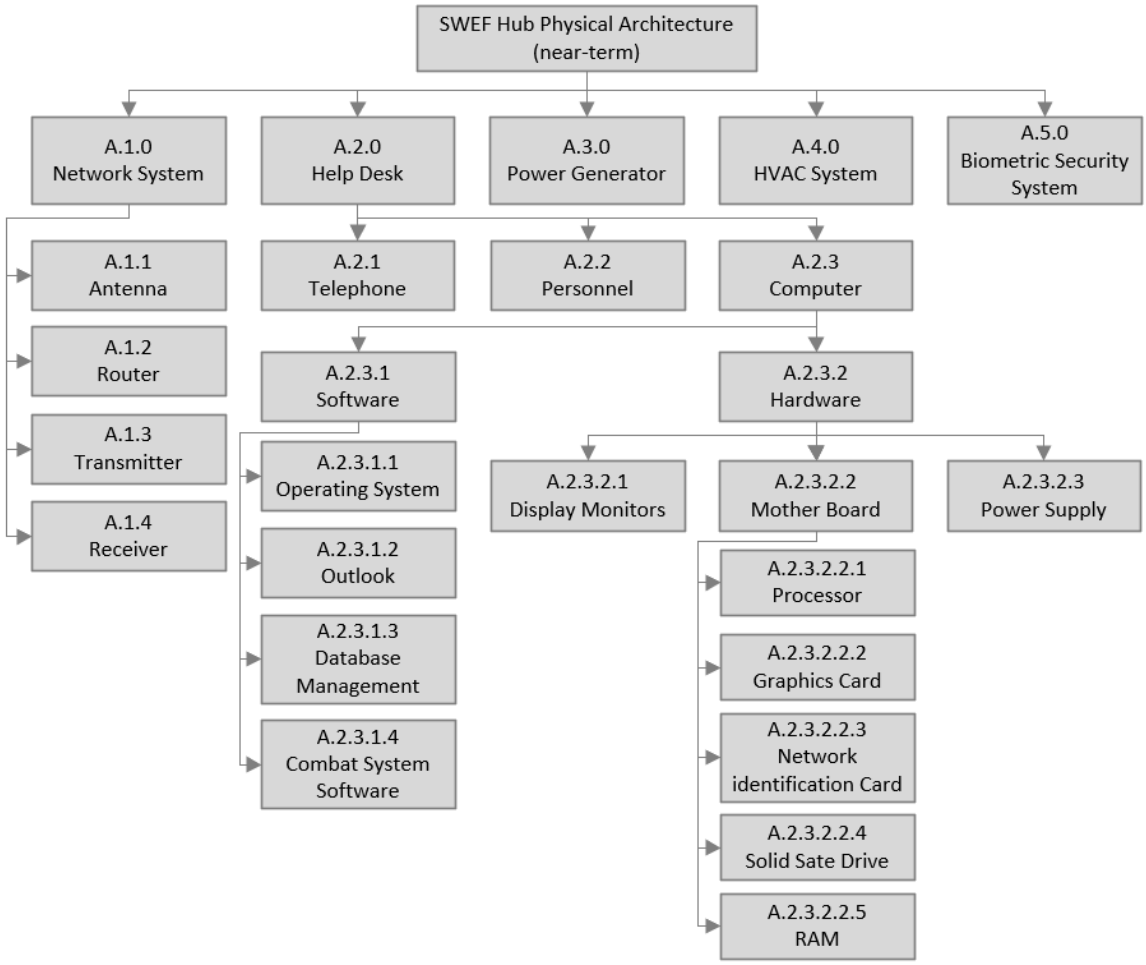


Figure 82. Physical Architecture Near-Term Diagram

3. Physical Architecture Long-Term Diagram Description

The long-term physical architecture is nearly identical to the near-term physical architecture. Level four below SWEF-Hub/help desk/computer/software, contains the only significant difference; that level contains a machine learning component with database management moved beneath it to level five. Combat system software, part of the physical architecture near-term diagram, is part of machine learning in the long-term diagram. See Figure 83 for details.

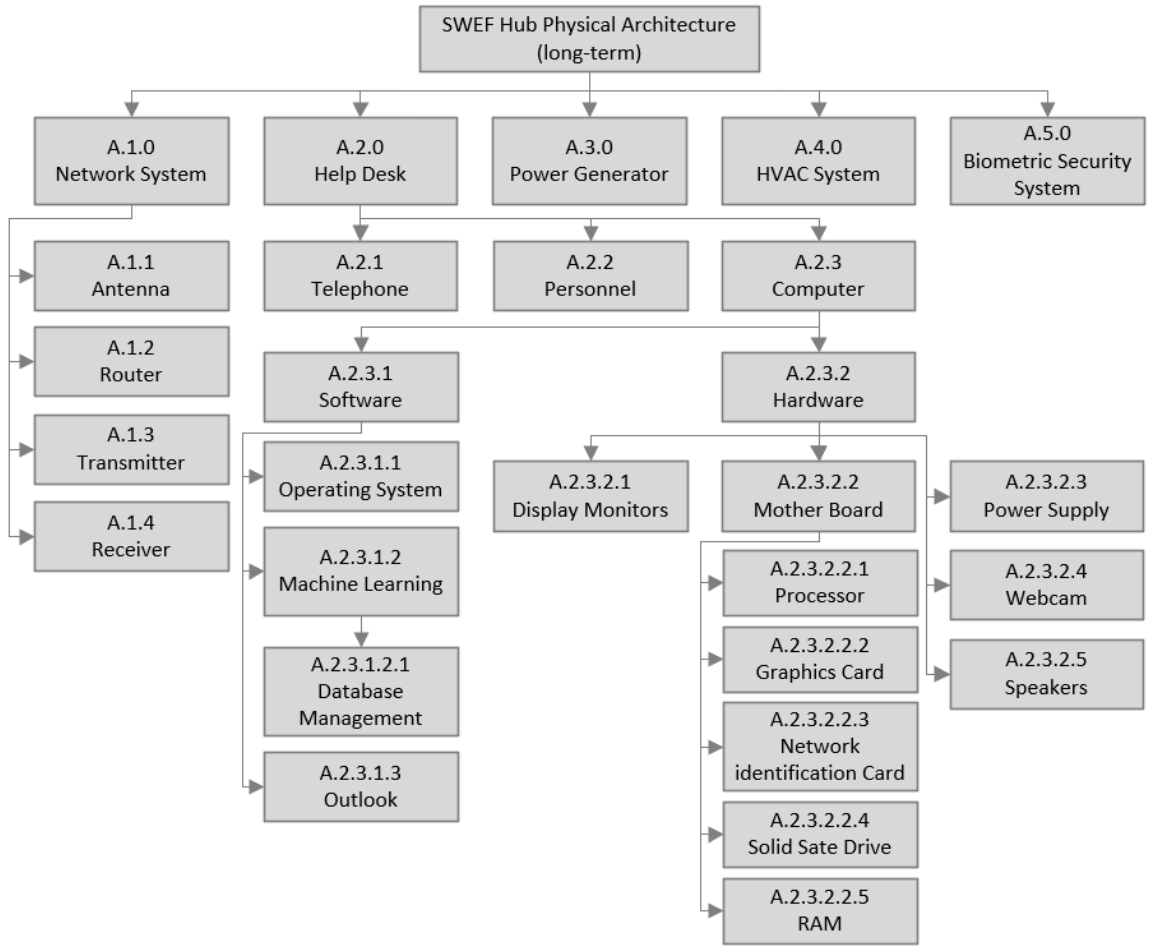


Figure 83. Physical Architecture Long-Term Diagram

G. THE INTERNAL AND EXTERNAL INTERFACES DIAGRAM DESCRIPTION

After the physical entities are identified, the internal and external interfaces are identified. Figure 84 shows the top-level interfaces that exist in the SWEF-Hub and the interface between the SWEF-Hub and the satellite. Figure 85 shows the top-level interfaces that exist in any secondary location and the interface between the secondary location and the satellite. The two figures together show the total top-level interfaces that exist when services are provided.

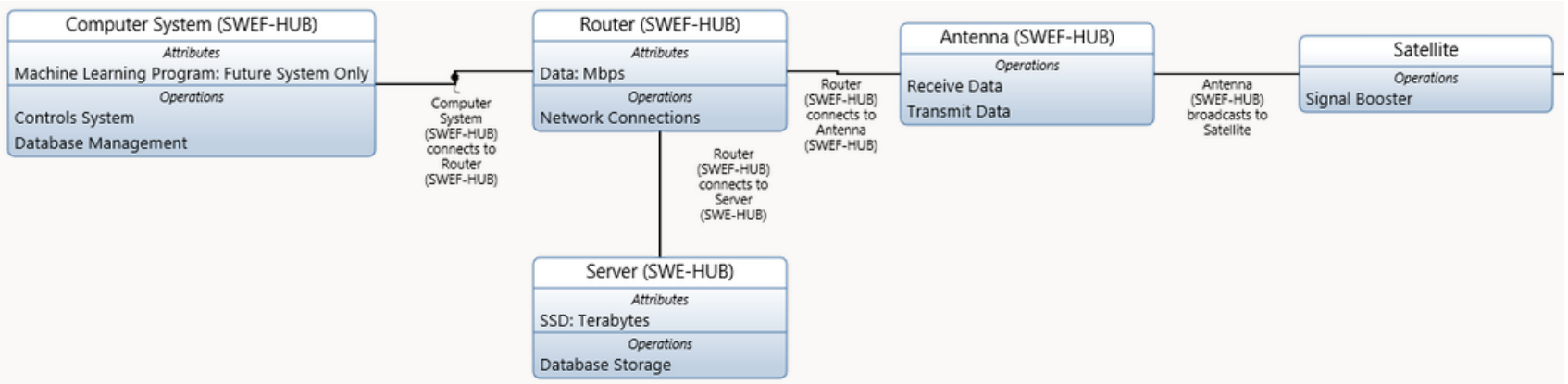


Figure 84. The Internal and External Interfaces Diagram Part A

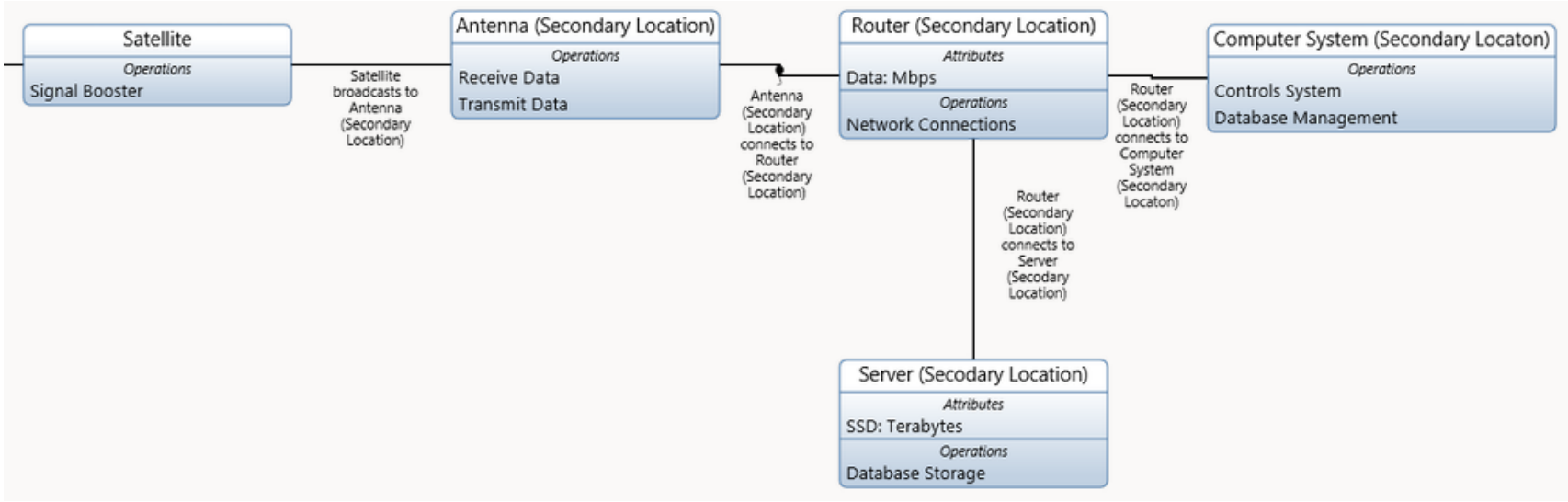


Figure 85. The Internal and External Interfaces Diagram Part B.

H. CONSTRAINTS

Constraints on a system are factors that affect the capabilities of a system but are not necessarily under the direct control of the system. The SWEF-Hub system has constraints relating to cyber security, military operations, staffing limits of both the SWEF-Hub and associated external entities, and problem complexity. These factors serve to limit or throttle the attainable objectives of the system. The following list shows some of the constraints that affect the SWEF-Hub:

- The SWEF-Hub must meet stringent cyber security requirements. Cyber security is an essential function; however, its' implementation tends to slow down computational processes and data transmission rates.

- Operational realities of military naval assets limit available communications windows as well as available communications bandwidths. The ship element determines whether operational tempo allows safe transmission of data.

- The SWEF-Hub will not be able to process all help-requests due to infrastructure and staffing limitations. Its capacity to process help-requests will depend on the type of problems and the total number of problems under consideration at any one moment. Some problems will be transferred to secondary locations for solution.

- Not every problem is going to have an immediate solution. Some problems can be solved quickly, while some require materials and/or complex solutions that inherently need more time for resolution.

I. RISK ANALYSIS

Risks are potential future events or conditions that may have a negative effect on achieving program objectives for cost, schedule, and performance (Office of the Deputy Assistant Secretary of Defense for Systems Engineering 2017). Because risk needs to be considered early in the systems engineering process, the team kept it under consideration from the start of the SWEF-Hub research collaboration. Information found within the

Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs (Office of the Deputy Assistant Secretary of Defense for Systems Engineering 2017) was referenced for this effort.

1. Risk Management

Figure 86 shows risk management as a continuous function. Identification is the first step to managing each of the identified risks and following the cycle is necessary for as many iterations as required to minimize the risk to the lowest possible levels.

Figure 86. Risk and Issue Management Process Overview. Source: Office of the Deputy Assistant Secretary of Defense for Systems Engineering (2017).

2. Risk Classification

Two risk classifications were identified from the SWEF-Hub research: technical and programmatic.

- Technical risks "... may prevent the end item from performing as intended or from meeting performance expectations."
- Programmatic risks "... can be associated with program estimating… program planning, program execution, communications, and contract structure" (Office of the Deputy Assistant Secretary of Defense for Systems Engineering 2017, 77).

3. Risk Analysis Goals

The risk analysis process goals include:

- Identify the risks.
- Analyze the risks identified to determine severity and probability of occurrence.
- Determine how to mitigate or control the risks.

For the analysis stage of the risk and issue process management, a consequence classification level is initially assigned and mitigating efforts are then determined in order to lower the consequence to an acceptable level through iterations of the risk and issue process management. Table 11 is the adapted severity table to assess risks.

Table 11. Risk Consequence Criteria. Adapted from the Office of the Deputy Assistant Secretary of Defense for Systems Engineering (2017).

Level	Impact	Schedule	Performance
1	Minimal	Minimal or no schedule impact.	Minimal impact.
2	Minor	Can meet objective and key event dates.	Design margins reduced within trade space.
3	Moderate	Can meet objective dates but key event dates will slip.	Design or supportability margins reduced.
4	Significant	Objective and key event dates will slip.	Significant performance impact; workarounds required to meet mission objective.
5	Critical	Will require a major schedule re-baselining.	Unable to meet mission objectives.

4. Risk Likelihood

Additionally, the probability of occurrence is just as important as the severity and is categorized by the probability that an event will occur given expected conditions. Table 12 is the adapted risk likelihood classification.

Table 12. Risk Likelihood Classification. Adapted from Office of the Deputy Assistant Secretary of Defense for Systems Engineering (2017).

Level	Likelihood	Probability of Occurrence
1	Not Likely	≤ 20%
2	Low Likelihood	≤ 40%
3	Likely	≤ 60%
4	Highly Likely	≤ 80%
5	Near Certainty	≤ 100%

5. Risk Assessment

Once the consequence classification level and likelihood classifications are determined, the specific risk can be classified by the chart depicted in Figure 87. This stop light chart of red, yellow, and green produce a graphically identified matrix of the categorized risk. Ultimately, the goal of risk assessment is to move any identified risk from red or yellow into a green zone (or as low as possible) by mitigation efforts and risk and issue management process iterations.

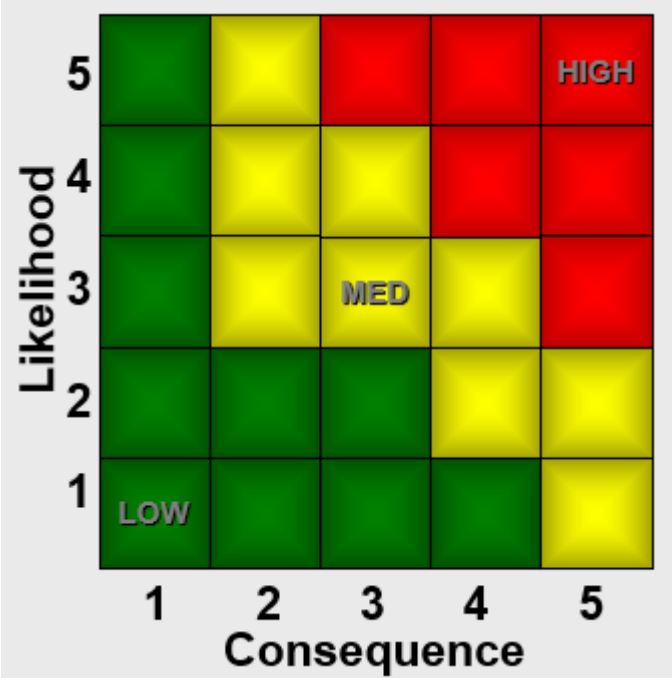


Figure 87. Risk Assessment Matrix. Adapted from Office of the Deputy Assistant Secretary of Defense for Systems Engineering (2017).

6. SWEF-Hub Risks

Technical and programmatic risks were determined and consolidated into two tables: Table 13 SWEF-Hub Technical Risks and Table 14 SWEF-Hub Programmatic Risks. Each risk number is followed by a description, likelihood, and consequence, with an initial risk assignment color (red, yellow, or green). A mitigation was developed, and a new mitigated risk assignment was assigned (red, yellow, or green). In each risk case,

mitigation resulted in a lower risk assignment. Continued evaluation and expert mitigation analysis could result in even lower risk as the project unfolds

The stakeholders specifically stated that we should not restrict development of the SWEF-Hub based on current technology limitations or estimated future advances. The emphasis taken from several conversations with stakeholders was that we should research what would be in the art of the possible should technology catch up with design. The SWEF-Hub requires technology which does not currently exist for the long-term solution both on the ship and within the SWEF-Hub.

Table 13. SWEF-Hub Technical Risks

Risk #	Description	Likelihood	Consequence	Initial Risk Assignment	Mitigation (Element changed)	Mitigated Risk Assignment
T1	Data formats do not follow a useful standard for collaboration.	Low	Significant	Yellow	Research and programming mapping required by computer software technicians. (Consequence – Minor)	Green
T2	Data transfer from an unclassified system to a classified system are reversed (information spillage).	Likely	Significant	Yellow	Computer software creating a one-way path from unclassified system to classified system with no reversal. (Likelihood – No)	Green
T3	Human-in-the-loop cannot articulate information.	Likely	Moderate	Yellow	Personnel training on supported systems, flow charts, and ISEA support equipment. (Likelihood – Low)	Green
T4	Machine learning system cannot articulate information.	Likely	Moderate	Yellow	Machine learning progressively learns, as the knowledge base is increased default to human-in-the-loop. (Likelihood – Low)	Green
T5	Cybersecurity is not achieved and maintained	Low	Critical	Yellow	Continuous and routine monitoring, software and hardware updates.	Green

Risk #	Description	Likelihood	Consequence	Initial Risk Assignment	Mitigation (Element changed)	Mitigated Risk Assignment
					Periodic intrusion testing (Likelihood – Not Likely)	
T6	Transmission paths become unavailable.	Low	Significant	Yellow	Install on site storage capacity (ship and shore side). (Consequence – Moderate)	Green
T7	Single hub entry/ exit location.	Likely	Significant	Yellow	Build into the system design a redundant location, routinely test. (Likelihood – Not Likely)	Green
T8	Satellite vulnerability.	Low	Significant	Yellow	Install on site storage capacity (ship and shore side). (Consequence – Moderate)	Green
T9	Hub data movement /analysis saturation.	Low	Significant	Yellow	Install on site storage capacity to allow for buffering. (Likelihood – Not Likely)	Green
T10	System configuration management onboard assets.	Likely	Moderate	Yellow	Automatic configuration database updates, train, and enact periodic configuration checks. (Likelihood – Not Likely)	Green
T11	Loss of incident tracking.	Likely	Moderate	Yellow	Enact an automatic incident ticketing system. (Likelihood – Not Likely)	Green
T12	Loss of database.	Likely	Critical	Red	Build into the system design a redundant off-site data storage backup system. Periodically run data comparison algorithms. (Likelihood – Not Likely)	Yellow

Table 14. SWEF-Hub Programmatic Risks

Risk #	Description	Likelihood	Consequence	Initial Risk Assignment	Mitigation (Element changed)	Mitigated Risk Assignment
P1	The team not being able to obtain relevant or enough information to deliver a useful product.	Likely	Critical	Red	Schedule, question, and present regular project status updates. Achieve routine direction. (Likelihood – Not Likely)	Yellow
P2	The team not being able to obtain concurrence from all stakeholders.	Likely	Significant	Yellow	Conduct regular stakeholder meetings and discussions on items of non-alignment. (Likelihood – Not Likely)	Green
P3	Misunderstanding stakeholder requirements.	Low	Significant	Yellow	Conduct regular stakeholder meetings and discussion on progress and requirements. (Likelihood – Not Likely)	Green
P4	Scope creep.	High	Moderate	Yellow	Conduct regular reviews and discussions with stakeholders the expected outcome of the SE process. (Likelihood – Low)	Green

J. SHOW THE RELATIONSHIP BETWEEN THE ARCHITECTURE AND DESIGN

The architecture and design are related by the idea that the architecture describes how a system should be structured while the design ensures that the architecture is achievable and capable of performing within the limits of the requirements. The architecture's structured actions are related to the design's physical elements due to the reasonable presumption that the physical elements will enable the action. (INCOSE 2015).

The system elements (physical elements: computer, antenna, software, etc.) are the parts of the architectural entities (models, views, viewpoints, diagrams, etc.). Allocation matrices are created to show the relationship between the elements of different architectural entities. For example, an allocation matrix will show the relationships of a functional flow-

block diagram to a physical block diagram. Tables 15 and 16 are representative examples of the allocation matrices based on the condition-based maintenance (CBM) near-term. Tables 35 through 50 in Appendix B show the complete set of relationships between the elements of functional entities vs the element of the physical entity. Each entity has a different functionality; however, some of the elements are the same or similar. In these matrices the "X" shows that a functional element is related to the corresponding physical element. These allocation matrices show that at least one physical element matches one functional element and vice versa (INCOSE 2015). The first set are the near-term allocation matrices and the second set are the long-term allocation matrices.

Table 15. CBM Near-Term

	A.1.1 Antenna	A.1.2 Router	A.1.3 Transmitter	A.1.4 Receiver	A.2.0 Help Desk	A.2.1 Telephone	A.2.2 Personnel	A.2.3 Computer	A.2.3.1 Software	A.2.3.1.1 Operating System	A.2.3.1.2 Outlook	A.2.3.1.3 Database Management	A.2.3.1.4 Combat System Software	A.2.3.1.5 Cyber Security Software	A.2.3.2 Hardware	A.2.3.2.1 Display Monitors	A.2.3.2.2 Mother Board	A.2.3.2.2.1 Processor	A.2.3.2.2.2 Graphics Card	A.2.3.2.2.3 Network Ident. Card	A.2.3.2.2.4 Solid State Drive	A.2.3.2.2.5 RAM	A.2.3.2.3 Power Supply	A.3.0 Power Generator	A.4.0 HVAC System	A.5.0 Biometric Security System
2.1 Scheduled Maintenance Performed	N/A																									
2.2 Transmit NOC Data to SWEF-HUB	X	X	X										N/A	X												
1.1 Stationed Monitoring	X	X	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X
2.3 Receive NOC	X	X	X	X			X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X			
2.4 Identify Tech Center					X		X	X	X	X		X			X	X	X	X	X	X	X	X	X			
2.5 Transmit NOC to Tech Center	X	X	X		X		X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X			
2.6 Receive NOC from SWEF-HUB	X	X		X				X	X	X	X	X		X	X	X	X	X	X	X	X	X	X			
2.7 Analyze NOC Data								X	X	X		X		X	X	X	X	X	X	X	X	X	X			
2.8 Transmit COA to SWEF-HUB	X	X	X				X			X	X			X	X	X	X	X	X	X	X	X	X			
2.9 Receive COA from Tech Center	X	X		X	X		X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X			
2.10 Identify Ship Element								X	X	X	X	X				X	X	X	X	X	X	X	X			
2.11 Transmit COA to Ship Element	X	X	X		X		X	X	X	X	X	X		X		X	X	X	X	X	X	X	X			

Table 16. CBM Near-Term (cont.)

	A.1.1 Antenna	A.1.2 Router	A.1.3 Transmitter	A.1.4 Receiver	A.2.0 Help Desk	A.2.1 Telephone	A.2.2 Personnel	A.2.3 Computer	A.2.3.1 Software	A.2.3.1.1 Operating System	A.2.3.1.2 Outlook	A.2.3.1.3 Database Management	A.2.3.1.4 Combat System Software	A.2.3.1.5 Cyber Security Software	A.2.3.2 Hardware	A.2.3.2.1 Display Monitors	A.2.3.2.2 Mother Board	A.2.3.2.2.1 Processor	A.2.3.2.2.2 Graphics Card	A.2.3.2.2.3 Network Ident. Card	A.2.3.2.2.4 Solid State Drive	A.2.3.2.2.5 RAM	A.2.3.2.3 Power Supply	A.3.0 Power Generator	A.4.0 HVAC System	A.5.0 Biometric Security System
2.12 Receive COA from SWEF-HUB	N/A																									
2.13 Implement COA																										
2.14 Complete COA																										
2.15 Transmit COA NOC to SWEF-HUB																										
2.16 Receive COA NOC	X	X		X			X			X	X	X	N/A	X	X	X	X	X	X	X	X	X	X			
2.17 Transmit COA NOC to Tech Center	X	X	X				X			X	X	X		X	X	X	X	X	X	X	X	X	X			
2.18 Receive COA NOC from SWEF-HUB	X	X		X			X			X	X	X		X	X	X	X	X	X	X	X	X	X			
2.19 Closeout Issue															X	X	X	X	X	X	X	X	X			
2.20 Transmit Message of Issue Closeout	X	X	X				X			X	X	X		X	X	X	X	X	X	X	X	X	X			
2.21 Receive Closeout Issue Message	X	X		X			X			X	X	X		X		X	X	X	X	X	X	X	X			
1.7 Store Data		X	X	X			X			X	X	X		X		X	X	X	X	X	X	X	X			

K. PRELIMINARY TECHNICAL PERFORMANCE MEASURES (TPMS)

Eventually the SWEF-Hub will rely on TPMs and activities to provide the stakeholders with measurable elements and data points to substantiate progress in the definition of the technical solution. TPMs will also provide a foundation to assess associated technical risk and issues that could eventually affect the proposed solution. INCOSE defines TPMs as “implementation measure of success that should be traceable to MOEs and MOS’s (operational perspective) with relationships defined” (INCOSE 2015, 59). Additionally, the Department of Defense Instruction (DoDI) 5000.02 requires the use of TPMs and metrics to assess program progress (Department of Defense [DOD] 2017); the SWEF-Hub system engineering process should adhere to the instruction. The SWEF-Hub’s RVTM documents the project’s requirements from a top-down perspective and ensures thoroughness in terms of traceability.

Properly established TPMs that have been planned accordingly serve as technical progress data points. They also help build stakeholder when traceability exists between the verification criteria. The fact that TPMs can also be tied to the assessment of risks helps to solidify this statement by providing the stakeholders with evidence to support decision making at the leadership level. Table 17 shows the TPMs and the related MOPs. The “XXX” in TPM-4 and TPM-15 designate values that will be assigned at a long-term date with consensus from the stakeholders.

Table 17. Technical Performance Measures and Related Measures of Performance

MOP ID	Measures Of Performance (MOP)	TPM ID	Technical Performance Measures (TPMs)
MOP-14	Percentage of data collected.	TPM-1	Percentage of lost data packets < 1%.
MOP-3	Percentage Gap identification.	TPM-2	100% accountability of lost data packets.
MOP-5	Data transfer rate.	TPM-3	Consistent (hourly avg.) transmission rates greater or equal to 1 Gbps.
MOP-2	Processor speed.	TPM-4	Processing speeds measured at XXX.
MOP-1	Number of status reports per number of data packages per day.	TPM-5	1:1 ratio of actual versus reported attacks.
MOP-1	Number of status reports per number of data packages per day.	TPM-6	1:1 ratio of status received versus status reported.
MOP-4	Recommendations per issue per day.	TPM-7	1:1 ratio of issues identified versus recommendations provided (if necessary).
MOP-6	Number of intrusions per days.	TPM-8	Number of security violations in fiscal year (FY).
MOP-13	Heat removal rate.	TPM-9	BTUs/Hr to maintain an hourly average temperature of 60 degrees Fahrenheit.
MOP-11	Frequency capacity.	TPM-10	Frequency capacity hourly averages.
MOP-5	Data transfer rate.	TPM-11	Consistent (hourly avg.) transmission rates (notional target is 10 Gbps)
MOP-1	Number of status reports per number of data packages per day.	TPM-12	1:1 ratio of status received versus status reported.
MOP-9	Data load-rate.	TPM-13	Number of objects transferred per second.
MOP-8	Software installation speed.	TPM-14	Upload/download/execute process total elapsed time.
MOP-2	Processor's speed.	TPM-15	Parallel/redundant channels with simultaneous processing speeds of XXX.
MOP-10	Protected attacks per total attacks per day.	TPM-16	100% successful blockage of cyber treats.
MOP-12	Ratio of identified/processed to reported threats.	TPM-17	1:1 ratio of threats identified versus threats reported.
MOP-7	Upgrade downtime.	TPM-18	Upgrade downtime no greater than 48 hours.

L. EVALUATE THE DIFFERENT ARCHITECTURE CANDIDATES (CONCEPTS)

Evaluation of different architectural candidates is normally an important step in the SE process. As an example, the team considered the use of a server at SWEF-Hub or a private cloud-based database to serve the database function. A SWEF-Hub-based server could provide an extra layer of security. Large amounts of data can require a large cloud-based database, a situation that can drive expenses very high. The team was unable to perform a cost analysis or a risk analysis on these candidates. Due to time constraints and the magnitude of this project, the team created only one candidate architecture for the SWEF-Hub. Additional effort would allow the creation of different architecture candidates for evaluation in order to select the most effective candidate architecture. The developed architecture presents all the elements needed for the SWEF-Hub to perform.

M. MANAGE THE ARCHITECTURE PROCESS AND THE ARCHITECTURE

The different materials and documents resulting from the architecture process are managed to ensure organization and traceability. They are organized for easy access and long-term reference. The physical architecture is reviewed to verify concurrence with the stakeholders' requirements, which is part of the traceability process. This ensures that no system requirement is ignored, and all the physical elements are necessary. This is a step that is performed after the physical elements are determined (INCOSE 2015). Table 18 is a list of system requirements used as reference for Tables 19, 20, and 21 describing the list of system requirements versus physical/software elements.

Table 18. System Requirements

SyR ID	System Requirements (FSyR)
SyR-1	The SWEF-Hub shall provide reports on detected attacks in real time to system owners.
SyR-2	The SWEF-Hub shall analyze data received for degraded performance to detect failure trends in order to provide automatic reports to system owners when patterns are detected.
SyR-3	The SWEF-Hub shall be able to provide status and summarized reports on data being transmitted as well as data received/archived to system owners.

SyR ID	System Requirements (FSyR)
SyR-4	The SWEF-Hub shall be capable of processing data by validating, sorting, summarizing, and aggregation in real time.
SyR-5	The SWEF-Hub shall identify gaps in data transmitted 99% of the time.
SyR-6	The SWEF-Hub shall maintain up to date security definitions and patching no more than two days old.
SyR-7	The SWEF-Hub shall provide automatic recommendations to system owners when systems are under test and after issues are identified.
SyR-8	The SWEF-Hub shall have interfaces/connectors to internally (within the building) exchange data with existing labs in different spaces.
SyR-9	The SWEF-Hub shall use a physical medium capable of high transmission rates >1gbs.
SyR-10	The Spaces within SWEF-Hub facilities shall include entry/exit physical security systems and measures for up to top secret level in accordance with security regulations as applicable.
SyR-11	The SWEF-Hub shall have a computer system to install software and process data.
SyR-12	The SWEF-Hub shall be able to identify supported and unsupported (gaps) platforms.
SyR-13	The SWEF-Hub shall have a communications system for emails, chat, audio, and video communications.
SyR-14	The SWEF-Hub shall utilize commercial products (COTs) for common data gathering, analyzing, and storing capabilities.
SyR-15	The SWEF-Hub architecture shall provide an extra 20% room for growth of hardware and software.
SyR-16	The SWEF-Hub shall have an open system capable of being upgraded with minimal impact or downtime.
SyR-17	The SWEF-Hub shall be capable of software installations of shipboard systems within one-hour period.
SyR-18	The SWEF-Hub shall have a computer system that consolidates hardware capabilities (e.g., server models) to reduce redundant hardware for multiple ship baselines.
SyR-19	The SWEF-Hub shall load external shipboard data into its shipboard systems within eight hours.
SyR-20	SWEF-Hub shall have a high-speed processor able to process at a minimum two sets of shipboard data at a given time.
SyR-21	The SWEF-Hub shall use hardware capable of supporting different shipboard systems.
SyR-22	The SWEF-Hub shall use commercial software (COT) to reduce the effort to operate shipboard baselines.
SyR-23	The SWEF-Hub shall have a processor capable of processing different data formats coming from fleet platforms (e.g., cruisers, destroyers, LCSs, LPDs, carriers).
SyR-24	The SWEF-Hub shall have an artificial intelligence-based ML system to provide distance support.
SyR-25	The SWEF-Hub shall load external shipboard data for analysis within eight hours.
SyR-26	The SWEF-Hub shall be able to load at a minimum two sets of external data for analysis.
SyR-27	The SWEF-Hub shall use hardware that is common across the fleet.
SyR-28	The SWEF-Hub shall have a combat system baseline software within its environment.

SyR ID	System Requirements (FSyR)
SyR-29	The SWEF-Hub shall have a cyber security system to provide continuous internal and external cyber defense capabilities.
SyR-30	The SWEF-Hub shall utilize commercial software (COTS) for real-time shipboard system monitoring.
SyR-31	The SWEF-Hub shall use fiber optics and ethernet cable infrastructure to provide secured internet connectivity.
SyR-32	The SWEF-Hub shall have an alert system to provide automated alerts to internal SWEF-Hub managers and approved NSWC PHD personnel when potential cyber threats are detected.
SyR-33	The SWEF-Hub shall contain an air conditioning system to maintain the space ventilated between 50–75 degrees Fahrenheit.
SyR-34	The SWEF-Hub shall have personnel (24/7) to provide distance support.
SyR-35	The SWEF-Hub shall have external interfaces for connections to laser weapon systems integration.
SyR-36	The SWEF-Hub shall have a server infrastructure for external data coming from fielded laser systems.
SyR-37	The SWEF-Hub shall provide the minimal shipboard ruggedized system hardware infrastructures.
SyR-38	The SWEF-Hub shall have redundant connection systems to provide redundant and secured connections to shipboard systems when providing distance support.
SyR-39	The SWEF-Hub shall use fiber optics and ethernet cable infrastructure for high speed communications.
SyR-40	The SWEF-Hub shall have a simulation system to recreate issues.
SyR-41	The SWEF-Hub shall have troubleshooting combat system simulators to recreate scenarios and extract data for analysis.
SyR-42	The SWEF-Hub shall analyze data from different combat systems.
SyR-43	SWEF-Hub shall have a communication system capable of supporting high communications rates that exceed 10Gbps.
SyR-44	The SWEF-Hub shall ensure 100% collection of transmitted data.
SyR-45	The SWEF-Hub shall incorporate a system architecture for supported platforms already residing in SWEF and for future planned systems.
SyR-46	The SWEF-Hub shall provide an expandable and adaptable infrastructure that is capable of integrating near future (0-3 years) planned capabilities.

.

Table 19. System Requirements versus Physical/Software Elements

Physical / Software Element	Network System				Help desk																Power generator	HVAC system	Biometric security system
							Computer																
							Software				Hardware												
																Mother board							
	Antenna	Router	Transmitter	Receiver	Telephone	Personnel	Operating system	Database management	Outlook	Machine Learning	Display monitors	Power supply	Cable assemblies	Webcam	Speakers	Processor	Graphics card	Network identification card	Solid state drive	Ram			
SyR-1							X	X	X		X						X						X
SyR-2							X	X	X	X	X						X						
SyR-3							X	X			X						X						
SyR-4							X	X								X							
SyR-5			X				X	X															
SyR-6																							X
SyR-7					X																		
SyR-8													X										
SyR-9	X		X																				
SyR-10																							X
SyR-11							X	X								X	X	X	X	X			
SyR-12							X	X		X													
SyR-13					X		X	X	X		X			X	X	X							X
SyR-14							X	X								X			X				
SyR-15	N/A																						

Table 20. System Requirements versus Physical/Software Elements (cont.)

Physical / Software Element	Network System				Help desk																Power generator	HVAC system	Biometric security system
							Computer																
							Software				Hardware												
																Mother board							
	Antenna	Router	Transmitter	Receiver	Telephone	Personnel	Operating system	Database management	Outlook	Machine Learning	Display monitors	Power supply	Cable assemblies	Webcam	Speakers	Processor	Graphics card	Network identification card	Solid state drive	Ram			
SyR-16	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X			X
SyR-17	X	X	X				X	X								X							X
SyR-18							X	X		X						X	X	X	X	X			X
SyR-19				X												X		X	X	X			
SyR-20																X							
SyR-21										X						X	X	X	X	X			
SyR-22							X	X															
SyR-23																X							
SyR-24							X	X	X	X													X
SyR-25	X	X		X																			
SyR-26							X	X								X		X	X	X			
SyR-27											X		X	X	X	X	X	X	X	X			
SyR-28							X	X	X	X													X
SyR-29																							X
SyR-30	X	X	X	X	X		X	X	X	X													X

Table 21. System Requirements versus Physical/Software Elements (cont.)

Physical / Software Element	Network System				Help desk																	Power generator	HVAC system	Biometric security system
							Computer																	
							Software				Hardware													
																Mother board								
	Antenna	Router	Transmitter	Receiver	Telephone	Personnel	Operating system	Database management	Outlook	Machine Learning	Display monitors	Power supply	Cable assemblies	Webcam	Speakers	Processor	Graphics card	Network identification card	Solid state drive	Ram			
SyR-31													X											
SyR-32																								X
SyR-33																							X	
SyR-34						X																		
SyR-35													X											
SyR-36																			X					
SyR-37													X									X		
SyR-38													X											
SyR-39													X											
SyR-40							X	X		X	X	X				X	X	X	X	X				X
SyR-41							X	X																
SyR-42							X	X		X		X				X		X	X	X				
SyR-43					X				X		X			X	X									
SyR-44	X	X		X															X					
SyR-45										X						X	X	X	X	X				
SyR-46							X	X		X						X	X	X	X	X				X

N. SWEF-HUB EQUIPMENT AND LOCATION RECOMMENDATION

The SWEF-Hub location requires enough space for an operator to monitor information as well as a computer server room to maintain the databases. Figure 88 is a recommendation for location due to the proximity to a vault area. Current occupation of the two rooms, 509A and 509B would require re-designation or an overall selection of an additional suitable location for the SWEF-Hub operations.

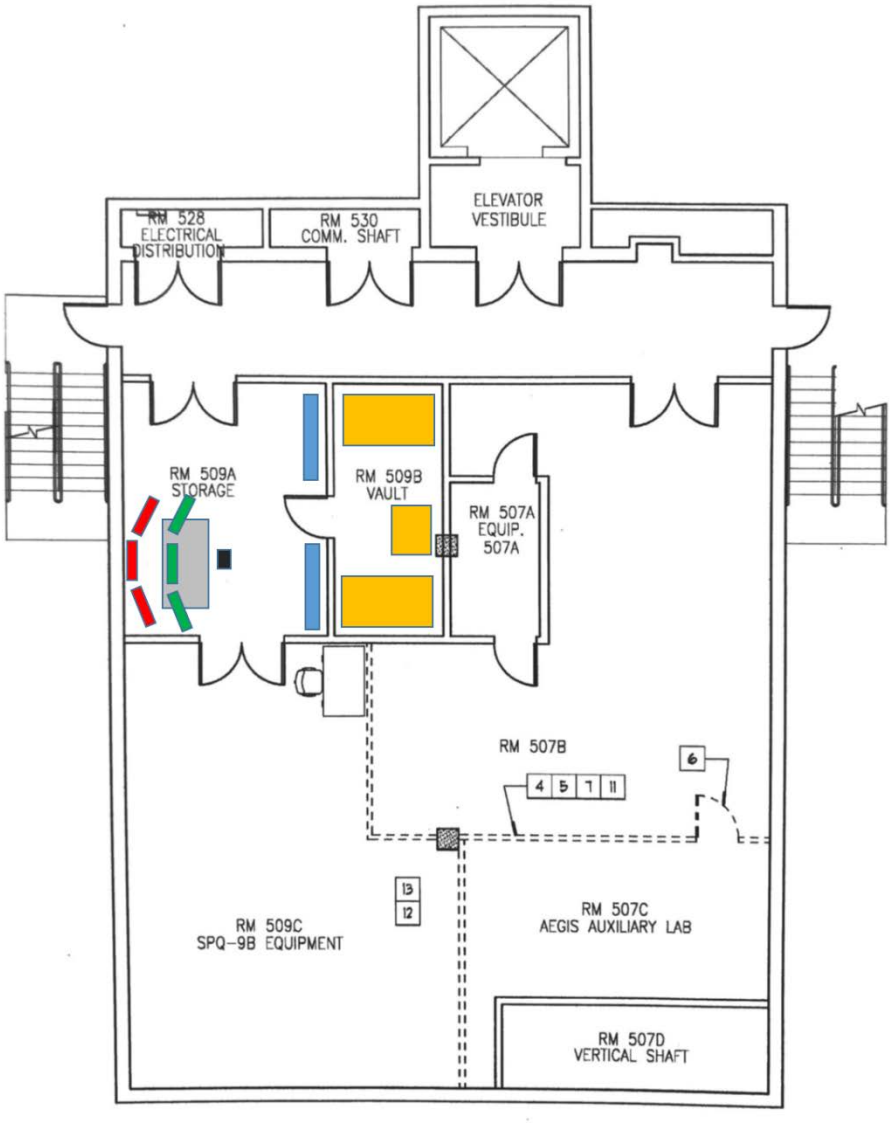


Figure 88. Recommended SWEF-Hub Location

The SWEF-Hub operation room could be contained within SWEF room 509A as the control room with the following equipment necessary as a minimum requirement:

1. A desk and chair for the watchstander. The desk requirement is to house both a NIPR and SIPR computer system with independent screens for each. In Figure 88, this is color coded grey and black.

2. A NIPR computer and screens (recommend 3 visual screens) to allow display of information, research, and tracking of incidents. In Figure 88, these are color coded green.

3. A SIPR computer and screens (recommend 3 visual screens) to allow display of information, research, and tracking of incidents. In Figure 88, these are color coded red.

4. Telephone lines with commercial and DSN access.

5. Two monitors (recommend LCS screen of at least 55 inches) with touch screen capability for ship combat system health status display. This display projects ship health status and location of all navy ships around the world. Touch screen facilitates a simple method for the selection of the desired ship and ship data on demand. Ship location data is fed from the NB Point Loma location of NIWC. Ship combat system health status is a conglomeration of data from the SWEF-Hub data base as well as other navy data bases. The ship combat system health status display information is pushed to various secure locations throughout NSWC PHD (A, L, S, Command department spaces) as well as other remote sites (TYCOM, NSWC, ISIC, etc.) desiring this information. In Figure 88, this is color coded blue.

1. Server Room Location

The SWEF-Hub data storage server room could be contained within SWEF room 509B. This space would house the required servers, processors, and necessary computer components for the SWEF-Hub to operate.

2. Antenna Location

Additionally, and not shown in Figure 88, the required satellite communication upload/download dishes are to be placed on the roof structure of the SWEF and connected to the SWEF-Hub data storage server room equipment.

3. Manning Recommendations

The SWEF-Hub manning recommendations include, for the watchstander, one person working per shift throughout the 24 hour/7 day week. This person is derived from the current 24/7 AegisTT/SSDS watch and LDSC watch groups. The watchstander is trained to identify equipment information and push the incoming information to the responsible technicians either onsite PHD or resident at other technical locations (NSWC/ NUWC/NIWC locations). The SWEF-Hub watchstander has the ability to contact departmental leadership at all times and SWEF-Hub supervisors have the ability and capability to visit the watch floor as necessary.

4. Environmental Considerations

The SWEF rooms 509A and 509B require heating, ventilation, and air conditioning equipment for equipment environmental requirements; sufficient power to run the equipment with either un-interruptible power supplies or backup generator power, NIPR/ SIPR communication lines, telephone lines, and communication lines to the satellite equipment placed on the roof of SWEF. Fire protection should be considered for server room protection; it should be easily accessible by the watchstander or automatically triggered upon meeting fire, heat, or smoke conditions. A secondary data storage location with scheduled and periodic backups, physically separate from the SWEF primary location, should be considered to prevent a total loss of data. The spaces require separate controlled access from main building access.

5. Near-Term and Long-Term Differences

The physical requirements within the SWEF-Hub room do not change between a near-term and long-term set up. Long-term requirements are internal to the computer operating systems and servers. Maintaining the current watches and configurations located at the AegisTT, LDSC, and Fleet Help Desk is required until the SWEF-Hub configuration is completed, tested, and verified to be fully operational. Recommendations include maintaining at least one of the current help desk locations as the primary backup throughout the life cycle of the SWEF-Hub as conditions warrant.

6. Communication Linkages

Figure 89 displays the communication flow paths for the SWEF-Hub. Internally to the SWEF location are a classified and unclassified network, typically SIPR and NIPR TCP/IP routing networks as well as SDREN and DREN. The unclassified network has the capability to be uploaded to the classified network but not in the reverse direction. In the near-term solution, shipboard data enters the SWEF-Hub via email. For the long-term solution, shipboard data enters the SWEF-Hub through classified satellite communications. The SWEF-Hub watchstander has the capability to display both SIPR and NIPR data as well as route the data to specific technical centers. Technical centers, as shown in Figure 89, are both onsite PHD and at various locations around the U.S. Additionally, the ship health display system is monitored and run by the watchstander in the SWEF-Hub. Data coming into the SWEF-Hub processors is from various sources consisting of CASREP data, ship location data, material status data, and other information as necessary. The SWEF-Hub ship health display is the driver for additional display systems throughout PHD and remote locations as necessary. Each of the remote ship health displays are envisioned to be touch screen displays.

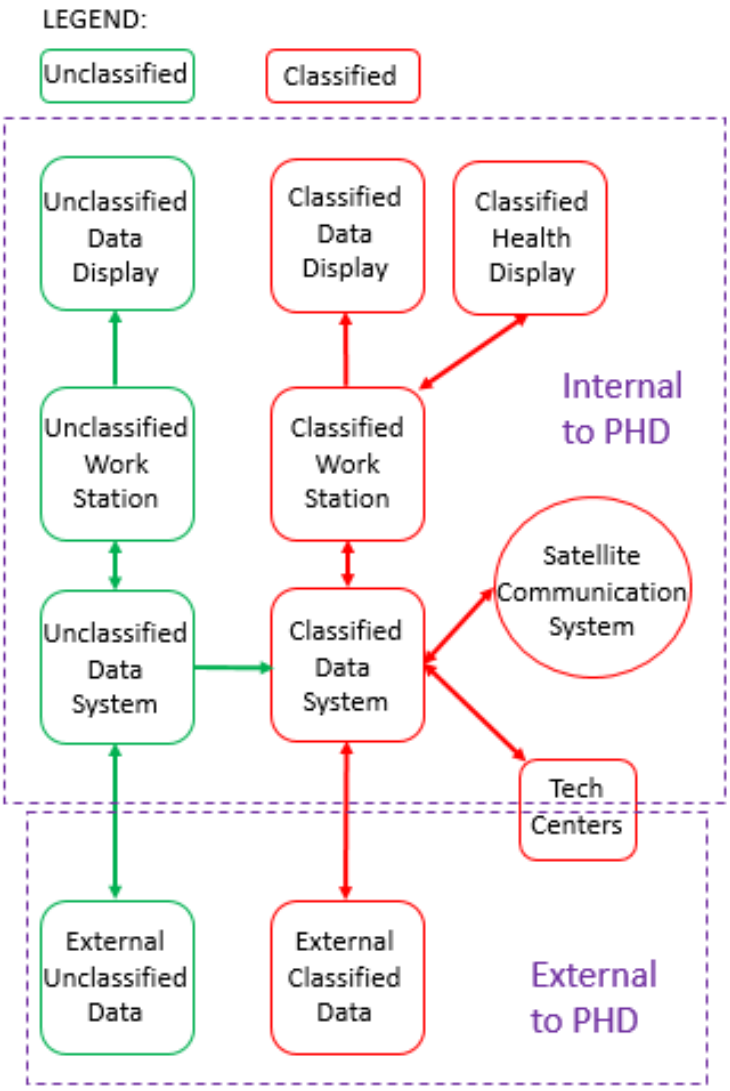


Figure 89. SWEF-Hub Communication Linkages

O. CHAPTER SUMMARY

The architecture definition was developed in Chapter V. Based upon the work accomplished in previous chapters, the system requirements were re-examined, questions about the long-term plans were answered, and a plan leading toward the architecture was developed. Viewpoints of the architecture were developed. Models and diagrams to display and assist in the development process were generated using tools such as Innoslate and Microsoft Excel. Efforts were made to show the relationship between the architecture and design, alternate architecture evaluation was discussed, and the management process for the architecture and the architecture process was discussed.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. SUMMARY AND CONCLUSIONS OF THE SWEF-HUB CAPSTONE PROJECT

In 2011, Phillip Baslisle (Vice Admiral, USN, retired), was called out of retirement by Commander, U.S. Fleet Forces to chair a surface fleet readiness review panel whose purpose was to address the navy's operational decline. A significant element in his findings was the Navy's decision to reduce manning and training, instigated at the same time that new programs with increasingly complex combat systems emerged, led to a decline in sailors' ability to operate, maintain, and sustain combat systems to the levels required in order to meet mission readiness requirements (Baslisle 2011).

Distance support (DS) efforts have been increasingly utilized throughout the fleet as a method for assisting and correcting complex technical issues. Communication paths between the fleet elements and the technical expertise of the ISEAs and SMEs have been through phone calls, email, and other web-based services; these paths are not always available to a ship at sea, nor are they always available at the most opportune periods (due to time zone differences). These communications paths allow the ISEAs and SMEs to provide information, troubleshooting efforts, recommendations, and problem resolutions to the fleet. To more effectively provide DS, the stakeholders desire a 24/7 center to receive information from the ships, to have the ability to push the information to various ISEA facilities and associated SMEs around the country for problem resolution, and to return the information or corrective action to the ship in an expeditious manner.

In this environment, the capability to repair equipment or, in some cases, predict equipment failures and perform preemptive maintenance actions, becomes necessary to support naval ships who are expected to sail into harm's way in areas around the globe. The ability to provide on-site technical subject matter experts (SMEs) is an increasingly costly solution that requires the utilization of a very limited resource.

Currently, system complexity requires SMEs to travel to a ship for problem identification and resolution due to the inability to receive accurate data through communication paths. The SWEF-Hub system architecture is designed to receive system data for the SMEs to work "in-house" and determine a corrective action. This capability

reduces the SME travel time, their time out of communications, their time spent working on a single issue, and the increasing costs associated with that method of problem resolution. Ship numbers are increasing, the number and complexity of combat systems is increasing, and the dependence of one combat system upon another is increasing all while resident shipboard knowledge is decreasing. The SME pool is limited but must serve an increasing demand. The result is that the amount of time available for an SME to resolve issues becomes shorter and shorter while budgets are both under more scrutiny and tightening. The adage "... to do more with less..." results in a requirement to utilize technological advances to our advantage that has never more apparent. The SWEF-Hub is envisioned to utilize technology to address the increasing demand for DS issues in the fleet while utilizing the limited SME core.

Additionally, reduced manning onboard ships results in a re-evaluation of the preventative maintenance system; the need to conduct routine maintenance to keep equipment operational. Preventive maintenance, while effective, is an expensive program with respect to manpower, material, and costs. The advent of technology to analyze system data for trends and abnormalities leads to an up and coming program within the U.S. Navy titled Condition-Based Maintenance (and Condition-Based Maintenance – Plus (CBM+) as the enhanced follow-on program). CBM calls for maintenance on equipment when the equipment has reached a condition requiring action. The SWEF-Hub has been architecturally designed to utilize the incoming data streams from a ship element to determine when those conditions are met and to inform the ship element as to necessary preventative maintenance.

This capstone project addresses the need for a centralized distance support solution with a combat systems focus. The stakeholders expressed their ideas and requirements for a capability to increase fleet readiness in an ever expanding and technologically intensive combat systems environment.

The team utilized an SE approach to clearly define an architecture for the SWEF-Hub. Meeting with the project stakeholders resulted in the SWEF-Hub context diagram presented in Chapter II of this report. The SWEF-Hub is designed to provide data management at its core and provide distance support, software modifications, data analysis,

and testing and evaluation of systems either on site or through additional ISEA sites. The use of additional in place ISEA sites was a critical requirement to avoid the costs associated with moving both personnel and equipment to the physical SWEF-Hub location. Instead, data transmission lines are utilized to move data to and from testing points. In the SWEF-Hub system, this data would be analyzed at the remote ISEA location and then returned to the SWEF-Hub for distribution back to the fleet asset of origin.

A future capability was considered where the SWEF-Hub would increase its scope to receive data concerning other, non-combat systems, passing that data on to the relevant ISEA facilities. These systems include hull, mechanical, and electrical (HM&E) systems. With this increase in scope, the SWEF-Hub would evolve into a complete fleet data hub. Further research would be required in order to entertain this possibility.

Fleet data transfers allow for the processing power of shore-based monitoring systems to analyze and evaluate trends between similar combat system units both across ship classes and across equipment baselines. This monitoring, conducted continuously (see Chapter V constraint section) vice having shipboard system diagnostic time along with ML analysis, leads to identifying and correcting problems before systems arrive at the point of complete failure or where an onboard technician or watchstander recognizes that something is wrong. Computer processing methods provide the ability to analyze the routine or semi-routine data from the fleet assets, compare it to designed system data, and monitor changes for possible degradation. This monitoring provides the premise for condition-based maintenance (described in Chapter V).

Machine learning and forecasting, along with logistics (materials, spare parts, maintenance assist modules, and routine repairables) already in place or on the way reduces the time to correction and increases fleet readiness. One such scenario would be incoming data monitored for a single fleet asset over the course of days or weeks, leading to an identifiable trend and an early repair notification to the asset. If the asset in question does not have the onboard logistics (through an automated review of onboard logistics records), the required element for repair could be shipped before the casualty occurs. Even if the casualty did occur prior to receiving the logistical element, it would already be on its way, resulting in reduced time to correction.

To meet the requirement of providing an overall asset combat systems health status, the team examined the ability to take input from existing systems and combine with fleet asset data to construct an asset health status. Utilizing fleet asset location data and reported equipment status from the NIWC location at NB Point Loma, constructing a combat systems table for each class of ship or sub-category of class of ship, and incoming fleet data, the SWEF-Hub will combine this information and export the results to remote locations. The data reporting would be through interactive presentation screens at locations throughout PHD or any other remote location as desired. This element of the SWEF-Hub requires further investigation as to the actual architecture necessary to construct this from NIWC information and SWEF-Hub data; however, the ability to collaborate with data from existing systems already exists.

A. NEAR-TERM VERSUS LONG-TERM NEEDS

The stakeholders agreed that a SWEF-Hub structure is a requirement to be established within the next three years. However, they also understood that technological advances would render a near-term SWEF-Hub design obsolete almost upon operation. The stakeholders asked for two models, a near-term capability and a model based ten-year out. The near-term capability would stand up utilizing current operations and technology and the out-year model would be unrestricted in design given the "art of what may be possible." Chapter V of this report provided two sets of architectural solutions to meet this requirement. While considering the ten-year model, a parallel model where the SWEF-Hub performs its functions as a hub for the maintenance and troubleshooting responsibilities of all NAVSEA entities.

There are currently multiple installed systems with the capability to provide reports off hull for both preventative as well as troubleshooting issues across the fleet. These tools include but are not limited to: Host Based Security System (HBSS), Security Information event management (SIEM) applications such as Splunk, Virtualized Data Transport Systems (VDTS) used for transporting CBM+ data from ships, and data collected from machinery propulsion control and monitoring systems (MPCMS) in other CBM+ systems. This information is already available but lacks a single common destination or node where

it can be collected, distributed, and analyzed. Currently each system owner is responsible for either extracting the data and/or analyzing it shipboard. This creates a delay between when the information is collected to when it is first seen by the SME and reviewed.

Using SWEF-Hub as a destination for the information already available and scattered throughout multiple fielded systems is a capability that can be stood up and accomplished within a reasonably short time frame. This would require the following tasks to be accomplished:

- Prepare the SWEF-Hub for operational use by performing any facility upgrades and/or repairs. This includes but is not limited to heating, ventilation, air conditioning (HVAC) repairs, electrical upgrades to accommodate future growth, and proper security requirements for an open secret space.

- Installation of both classified and unclassified network drops for external connections. These would be the interface for communication between ships and SWEF-Hub as well as other external groups.

- Procurement of hardware including lab equipment (e.g., cabinets, tables, chairs), servers, human machine interface (HMI) equipment, power supplies, network hardware (e.g., switches, routers), firewalls, etc. A hardware suite would be required for both classified and unclassified enclaves since data can also be transferred for unclassified systems.

- Procurement of software licenses for operating systems (for both classified and unclassified enclaves) as well applications to support minimum SWEF-Hub functionality.

- Laboratory accreditation for use of equipment which would include risk management framework (RMF) package for the use of SWEF-Hub.

Once the SWEF-hub is established and operational, systems that are currently transmitting data to NSWC PHD can start to update their connections to send the data to

SWEF-Hub. This would require the previous tasks to be completed in order to avoid jeopardizing the systems accreditation when connecting to the SWEF-Hub. The immediate effort would be to provide a common area (SWEF-Hub) to receive data. Local ISEAs would still be required to analyze the data once at SWEF-Hub manually or by their respected applications as needed. Communication with external systems would not be automatic in this phase.

Long-term needs would involve expanding the capabilities established by the near-term needs description above. This would include adding artificial intelligence capability to the SWEF-Hub to automatically assess data being received in real time to determine potential issues, discrepancies in data, alerts for potential hardware issues, trend analysis, and metrics collection. Alerts would be provided to the appropriate system owners both local to NSWC PHD and external systems. Having the SWEF-Hub infrastructure established and already in use would provide the platform to socialize the capabilities SWEF-Hub provides to programs supported within NSWC PHD as well as external systems. One of the goals involves having additional external systems start utilizing the SWEF-Hub as the central location for data from across the fleet to be transmitted for supporting system owners. This will help to alleviate system owners needs for actively monitoring their respected systems within their own facilities, which might be limited in capabilities when compared to that being offered within the SWEF-Hub. Additional long-term needs would also involve near real time bi-directional communication between the SWEF-Hub and fleet assets. This would include being able to push patches, new software builds, updated configurations, and adaptation data to systems on ships connected to the SWEF-Hub. This will reduce the amount of time that it takes for these types of changes to make it to the shipboard systems. In addition to fielded platforms, new programs that are still in the requirements phase could be updated to include requirements for connectivity to external sites (e.g., SWEF-Hub) for transmitting system data (e.g., logs, metrics). This capability could be tested by having those new system connected and send data to SWEF-Hub to verify their requirements. This will also ensure that when the systems are delivered, the infrastructure and connectivity is already in place to be in used as soon as the system is delivered to the Navy.

B. AREAS FOR FURTHER RESEARCH

In addition to the recommendations presented for the near-term system needs and those for future system needs, there are multiple opportunities that can be explored for future research to take advantage of the capabilities SWEF-Hub can provide. This includes:

- Expanding shipboard system external reporting to more than just the combat system, but to both unclassified and classified systems onboard hulls.

- Development of a bi-directional secure common interface within ships that can serve as the intermediate application for collecting data from the ships internal systems to send to the SWEF-Hub. Applications should be able to monitor available bandwidth and reduce transmission rates to avoid overloading external communications. This should be automatic, without the need for user intervention, and be applicable for both unclassified and classified enclaves regardless of the platform in use.

- Develop application program interfaces (API) for SWEF-Hub ML to be able to query and receive status from Navy wide systems in place for supporting the fleet. This includes Navy supply systems, logistic systems, configuration management systems, and patch repositories for both commercial systems as well as ISEA owned systems. These API's will provide the means for the SWEF-Hub artificial intelligence-based systems (such as ML) to communicate with those systems and use machine learning to compare what ships platforms are reporting and to provide preventative recommendations by using all available information across the enterprise.

- Investigate ISEA of the Future inputs for inclusion into the SWEF-Hub architecture. Across the NAVWAR and NAVSEA communities to are several collaborative research efforts regarding technologies to increase fleet readiness in both short term (less than three years) and long-term (greater than three years) efforts. These include (Mann 2019): additive manufacturing, advanced repair, CBM+, combat system virtualization, data analytics,

installation and modernization dashboard, model-based product support, sensor deployment prognostics, virtual reality, and virtual technical assists.

C. FINAL COMMENTS

There is a tremendous amount of potential for the SWEF-Hub to grow and increase its reach throughout the fleet. Some of these technologies mentioned are already under consideration for implementation but are not yet mature enough for near-term implementation. Regardless, we as government servants should create and foster an innovative culture that is aware of and conversant in the latest technologies and engages private industry with our long-term goals and vision to enable the development of future technology with a focus on combat capability.

In conclusion, the SWEF-Hub team strongly recommends the stakeholders proceed towards acquiring a SWEF-Hub Distance Support facility. This report is the beginning of the investigative research into the SWEF-Hub system and provides an architecture upon which to build. The team, as a final recommendation, urges the stakeholders to pass our findings to a subsequent cohort for continuation of the research.

APPENDIX A. REQUIREMENTS VERIFICATION AND TRACEABILITY MATRIX (RVTM)

This appendix displays the complete requirements verification and traceability matrix (RVTM). Due to the large size of the matrix, it is split up both horizontally and vertically. The matrix shows traceability from the initial stakeholders and their perceived needs through stakeholder requirements, functional requirements, the generation of system requirements, and all the way down to verification and validation criteria.

The first figure is a map showing the table numbers corresponding to each section of the horizontal and vertical slices of the matrix. The following pages show the portions of the matrix in a format large enough to see clearly.

Each horizontal slice of the matrix is broken into a set of three pages. Each page in the set shows the stakeholder ID, the stakeholder, and their description as a reference. The first page in the set traces from the stakeholders and their initial perceived (primitive) needs, through the determination of effective needs and stakeholder requirements. The second page continues on through the generation of functional and non-functional requirements that make up the stakeholder requirements, the determination of the reasonable MOEs that indicate that the functional and non-functional requirements have been met, and end with the system requirements (functional) and non-system requirements (non-functionally related). The third page in the set traces on through the identification of MOPs and TPMs that are necessary to show that the system performs its functions acceptably and ends with a listing of the validation criteria/methodology.

Table 22. RVTM Map

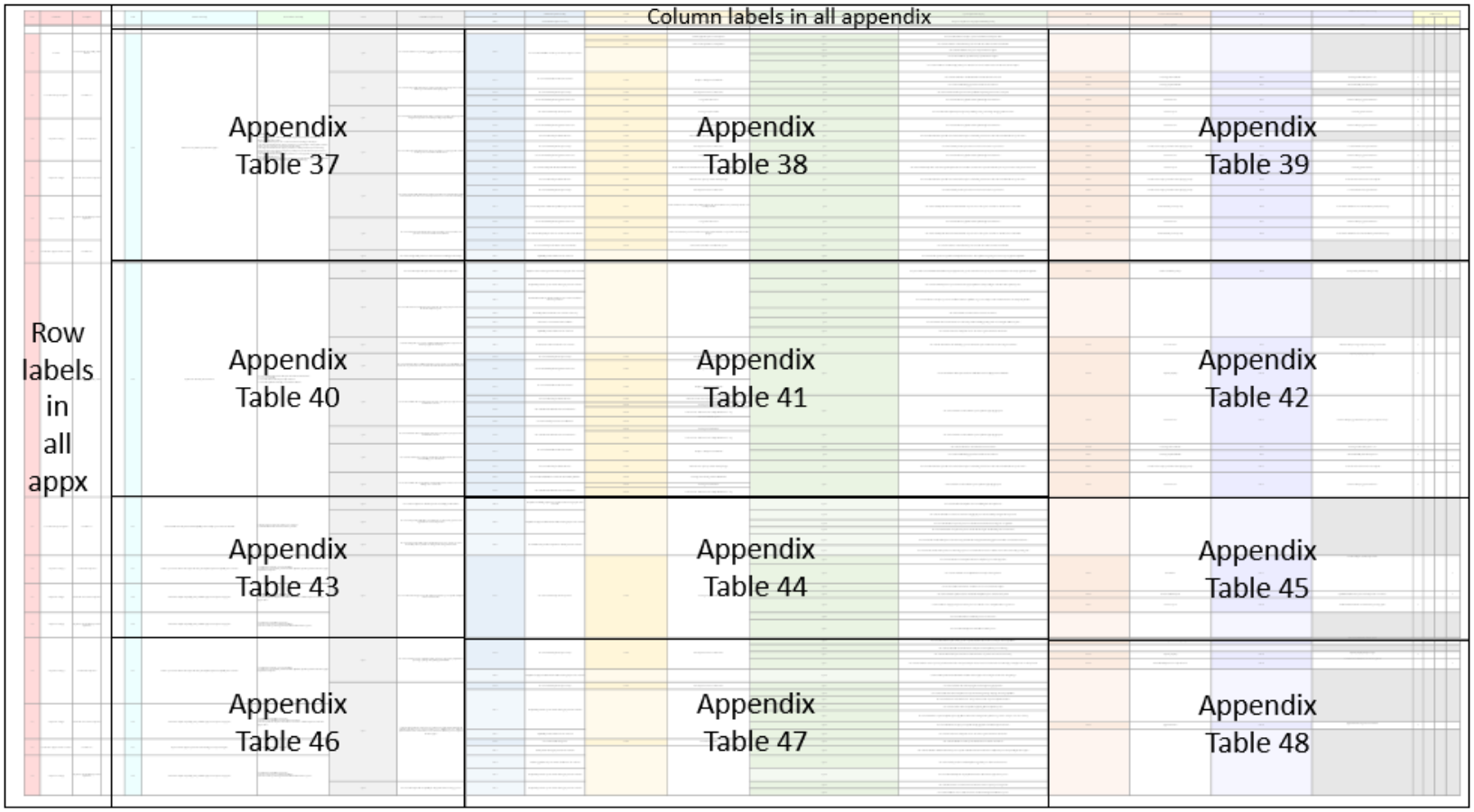


Table 23. Top Slice, Left Side of RVTM Map

St ID	Stakeholder	Description	PN ID	Primitive Needs (PN)	EN ID. Effective Needs (EN)	StR ID	Stakeholders Requirements (StR)
St-5	NSWC PHD	Overall Command where facility will be located.	PN-5	Innovate the Navy combat system distance support.	Statement Of Work (SOW) 1. Develop a re-design of Surface Warfare Engineering Facility (SWEF) as a central hub for Navy combat systems distance support. 2. This design would incorporate ISEA of the future focused technologies and concepts. 3. The design will enable distance support practitioners to securely (Cyber Security) collect real time Combat Systems Health and Status Data from deployed ships. 4. The design will enable distance support practitioners to analyze and interpret the data using advanced predictive data analysis (AI/Big Data) techniques to provide sailors with preventative or corrective action recommendations. 5. The design will enable distance support practitioners to securely provide real time combat systems status to Fleet decision makers. 6. The design will enable distance support practitioners to provide distance support recommendations to the fleet from secondary locations across the command (redundancy).	SyR-0	The SWEF-Hub shall be a Navy combat systems distance support center to provide support to the fleet.
St-1	NSWC PHD Lead System Engineer	PHD Code 203				SyR-1	The SWEF-Hub design shall enable distance support practitioners to securely collect real time combat system health data from deployed ships.
St-4	A Department Manager	Air Dominance Department				SyR-2	The SWEF-Hub design shall enable distance support practitioners to analyze and interpret data using advanced predictive data analysis (AI/Big Data) techniques.
St-2	L Department Manager	Littoral and Strike Warfare Department				SyR-3	The SWEF-Hub design shall enable distance support practitioners to securely provide real time combat systems status to fleet decision makers.
St-6	S Department Manager	Ship Defense and Expeditionary Warfare Department				SyR-4	The SWEF-Hub design shall enable distance support practitioners to provide distance support recommendations to the fleet from secondary locations across the command (redundancy).
St-3	PHD Distance Support Customer Advocate	PHD Code 206				SyR-5	The SWEF-Hub design shall enable distance support practitioner to provide sailors with preventive or corrective action recommendations.
						SyR-14	The SWEF-Hub design shall provide ISEA of the future focused technologies and concepts.

Table 24. Top Slice, Center of RVTM Map

St ID	Stakeholder	Description	FR ID	Functional Requirements (FRs)	MOE ID	Measure Of Effectiveness (MOE)	SyR ID	System Requirements (FSyR)
			NFR ID	Non-Functional Requirements (NFR)	NA	MOE not applicable	NSyR ID	Non-System Requirements (NSyR) (Non-functionally related)
St-5	NSWC PHD	Overall Command where facility will be located.	FR-0.0	The SWEF-Hub shall facilitate combat systems distance support in real time.	MOE-1	Ratio of supported requests to total requests.	SyR-11	The SWEF-Hub shall have a computer system to install software and process data.
					MOE-2	Ratio of resolved problems to total problems.	SyR-13	The SWEF-Hub shall have a communications system for emails, chat, audio, and video communications.
							SyR-24	The SWEF-Hub shall have an AI system to provide distance support.
							SyR-34	The SWEF-Hub shall have personnel (24/7) to provide distance support.
							SyR-41	The SWEF-Hub shall have troubleshooting combat system simulators to recreate scenarios and extract data from them for analysis.
St-1	NSWC PHD Lead System Engineer	PHD Code 203	FR-1.1	The SWEF-Hub shall collect health and status data.	MOE-4	Complete vs incomplete data collection.	SyR-44	The SWEF-Hub shall ensure succesful collection of transmitted data is near 100%.
							SyR-5	The SWEF-Hub shall identify gaps in data transmitted 99% of the time.
			FR-1.4	The SWEF-Hub shall implement cyber security.	MOE-8	Ratio of protected attacks to total attacks.	SyR-6	The SWEF-Hub shall maintain up to date security definitions and patching no more then two days old.
			FR-1.5	The SWEF-Hub shall implement high data transfer rates.	MOE-9	Average data transfer rates.	SyR-9	The SWEF-Hub shall use a physical medium capable of high transmission rates.
			FR-1.2	The SWEF-Hub shall analyze and interpret data.	MOE-6	Percentage of processed data.	SyR-4	The SWEF-Hub shall be capable of processing data by validating, sorting, summarizing, and aggregation in real time.
St-4	A Department Manager	Air Dominance Department	FR-1.5	The SWEF-Hub shall implement high data transfer rates.	MOE-9	Average data transfer rates.	SyR-9	The SWEF-Hub shall use a physical medium capable of high transmission rates.
			FR-1.3	The SWEF-Hub shall report health and status.	MOE-7	Number of status reports per number of data packages.	SyR-3	The SWEF-Hub shall be able to provide status and summarized reports on data being transmitted as well as data received/archived to system owners.
			FR-1.4	The SWEF-Hub shall implement cyber security.	MOE-8	Ratio of protected attacks to total attacks.	SyR-1	The SWEF-Hub shall provide reports on detected attacks in real time to system owners.
			FR-1.5	The SWEF-Hub shall implement high data transfer rates.	MOE-9	Average data transfer rates.	SyR-9	The SWEF-Hub shall use a physical medium capable of high transmission rates.
St-2	L Department Manager	Littoral and Strike Warfare Department	FR-2.2	The SWEF-Hub shall provide advanced situational awareness.	MOE-12	Number of incidents that situational awareness was provided vs the number of complete data packages.	SyR-2	The SWEF-Hub shall analyze data received for degraded performance to detect failure trends in order to provide automatic reports to system owners when patterns are detected.
			FR-1.3	The SWEF-Hub shall report health and status.	MOE-7	Number of status reports per number of data packages.	SyR-3	The SWEF-Hub shall be able to provide status and summarized reports on data being transmitted as well as data received/archived to system owners.
			FR-1.4	The SWEF-Hub shall implement cyber security.	MOE-8	Ratio of protected attacks to total attacks.	SyR-1	The SWEF-Hub shall provide reports on detected attacks in real time to system owners.
St-6	S Department Manager	Ship Defense and Expeditionary Warfare Department	FR-2.1	The SWEF-Hub shall provide technical and specialized support and recommendations.	MOE-11	Number of incidents where technical and specialized support and recommendations were provided by the hub vs the secondary location.	SyR-7	The SWEF-Hub shall provide automatic recommendations to system owners when systems are under test and after issues are identified.
			FR-1.5	The SWEF-Hub shall implement high data transfer rates.	MOE-9	Average data transfer rates.	SyR-9	The SWEF-Hub shall use a physical medium capable of high transmission rates.
			FR-2.3	The SWEF-Hub shall provide preventive or corrective action recommendations.	MOE-13	Number of occasions that preventive and corrective action recommendations were provided vs the number of data packages.	SyR-7	The SWEF-Hub shall provide automatic recommendations to system owners when systems are under test and after issues are identified.
St-3	PHD Distance Support Customer Advocate	PHD Code 206	FR-2.5	The SWEF-Hub shall provide audio or video communication.	MOE-15	SWEF-Hub can communicate via audio/video - yes/no.	SyR-13	The SWEF-Hub shall have a communications system for emails, chat, audio, and video communications.
			NFR-2	Expandability shall be considered at the SWEF-Hub.			SyR-46	The SWEF-Hub shall provide an expandable and adaptable infrastructure that is capable of integrating near future (0-5 years) planned capabilities.

Table 25. Top Slice, Right Side of Map

St ID	Stakeholder	Description	MOP ID	Measures Of Performance (MOP)	TPM ID	Technical Performance Measures (TPMs)	Validation Criteria			
			NA	MOP not applicable	NA	TMP	A	D	I	T
St-5	NSWC PHD	Overall Command where facility will be located.								
St-1	NSWC PHD Lead System Engineer	PHD Code 203	MOP-14	Percentage of data collected.	TPM-1	Percentage of lossed data packets < 1%.	X			
			MOP-3	Percentage Gap identification.	TPM-2	100% accountability of lossed data packets.	X			
			MOP-5	Data transfer rate.	TPM-3	Consistent (hourly avg.) transmission rates.	X			
			MOP-2	Processor's speed.	TPM-4	Processing speeds measured.	X			
St-4	A Department Manager	Air Dominance Department	MOP-5	Data transfer rate.	TPM-3	Consistent (hourly avg.) transmission rates.	X			
			MOP-1	Number of status reports per number of data packages per day.	TPM-5	1:1 ratio of actual versus reported attacks.				X
			MOP-5	Data transfer rate.	TPM-3	Consistent (hourly avg.) transmission rates.	X			
			MOP-2	Processor's speed.	TPM-4	Processing speeds measured.	X			
St-2	L Department Manager	Littoral and Strike Warfare Department	MOP-1	Number of status reports per number of data packages per day.	TPM-6	1:1 ratio of status received versus status reported.				X
			MOP-1	Number of status reports per number of data packages per day.	TPM-5	1:1 ratio of actual versus reported attacks.				X
St-6	S Department Manager	Ship Defense and Expeditionary Warfare Department	MOP-4	Recommendations per issue per day.	TPM-7	1:1 ratio of issues identified versus recommendations provided (if necessary).				X
			MOP-5	Data transfer rate.	TPM-3	Consistent (hourly avg.) transmission rates.	X			
			MOP-4	Recommendations per issue per day.	TPM-7	1:1 ratio of issues identified versus recommendations provided (if necessary).				X
St-3	PHD Distance Support Customer Advocate	PHD Code 206								

Table 26. Level 2 Slice, Left Side of Map

St ID	Stakeholder	Description	PN ID	Primitive Needs (PN)	EN ID. Effective Needs (EN)	StR ID	Stakeholders Requirements (StR)
St-5	NSWC PHD	Overall Command where facility will be located.	PN-6	Requirements for facility and sustainment.	10. Secure classified information in lab spaces and other internal locations. 11. HVAC system capable. 12. SWEF-Hub and internal lab spaces fully connected. 13. SWEF-Hub capable of connecting to external sites and fleet.	SyR-17	The SWEF-Hub shall provide spaces that meet top secret space requirements.
						SyR-18	The SWEF-Hub architecture shall be designed to maximize the use of agency internal resources for common shipboard systems.
						SyR-21	SWEF-Hub shall provide HVAC systems capable of maintaining adequate temperature for laboratory equipment (hardware).
						SyR-6	The SWEF-Hub shall be able to stablish connectivity with SWEF spaces, external buildings, sites, and the fleet to provide and receive classified and unclassified data and information in real time.
						SyR-7	The SWEF-Hub shall be able to exchange data with other SWEF spaces up to top secret level classification in real time.
						SyR-9	The SWEF-Hub shall be able to communicate with other SWEF spaces up to top secret level classification in real time.
						SyR-8	The SWEF-Hub shall be able to exchange classified data and information in real time with external buildings, sites, and the fleet.
						SyR-10	The SWEF-Hub shall be able to communicate classified information in real time with external buildings, sites, and the fleet.

Table 27. Level 2 Slice, Center of Map

St ID	Stakeholder	Description	FR ID	Functional Requirements (FRs)	MOE ID	Measure Of Effectiveness (MOE)	SyR ID	System Requirements (FSyR)
			NFR ID	Non-Functional Requirements (NFR)	NA	MOE not applicable	NSyR ID	Non-System Requirements (NSyR) (Non-functionally related)
St-5	NSWC PHD	Overall Command where facility will be located.	NFR-6	Compliance with PHD security protocols shall be an integral part of the SWEF-Hub.			SyR-10	The Spaces within SWEF-Hub facilities shall include entry/exit physical security systems and measures for up to top secret level in accordance with security regulations as applicable.
			NFR-1	Comparability with other systems shall be an integral part of the SWEF-Hub.			lSyR-45	The SWEF-Hub shall incorporate a system architecture for supported platforms already residing in SWEF and for future planned systems.
			NFR-11	Consolidation of hardware shall be considered at the SWEF-Hub to eliminate unnecessary hardware.			SyR-18	The SWEF-Hub shall have a computer system that consolidates hardware capabilities (e.g. server models) to reduce redundant hardware for multiple ship baselines.
			NFR-8	Commonality shall be considered at the SWEF-Hub as necessary.			SyR-27	The SWEF-Hub shall use hardware that is common across the fleet.
			NFR-9	Connection to SWEF-Hab labs shall be stablished.			SyR-8	The SWEF-Hub shall have interfaces/connectors to internally (within the building) exchange data with existing labs in different spaces.
			NFR-2	Expandability shall be considered at the SWEF-Hub.			SyR-15	The SWEF-Hub architecture shall provide a extra 20% room for growth of hardware and software.
			NFR-12	Personnel factors shall be considered at the SWEF-Hub.			SyR-33	The SWEF-Hub shall contain an air conditioning system to maintain the space ventilated between 50-70 degrees Fahrenheit.
			FR-1.4	The SWEF-Hub shall implement cyber security.	MOE-8	Ratio of protected attacks to total attacks.	SyR-39	The SWEF-Hub shall use fiber optics and ethernet cable infrastructure for high speed communications.
			FR-1.5	The SWEF-Hub shall implement high data transfer rates.	MOE-9	Average data transfer rates.		
			FR-1.1	The SWEF-Hub shall collect health and status data.	MOE-4	Complete vs incomplete data collection.		
			FR-1.3	The SWEF-Hub shall report health and status.	MOE-7	Number of real time status reports vs number of data packages.	SyR-43	The SWEF-Hub shall have a communication system capable of supporting high speed.
			FR-3.0	The SWEF-Hub shall troubleshoot software and hardware.	MOE-16	Percentage of resolved issues.		
					MOE-17	Mean corrective maintenance time ($M^{bar}ct$). (Blanchard 2011, 412)		
			FR-4.0	The SWEF-Hub shall provide software modifications.	MOE-20	Successful modification - yes/no.		
			FR-3.0	The SWEF-Hub shall troubleshoot software and hardware.	MOE-16	Percentage of resolved issues.	SyR-43	The SWEF-Hub shall have a communication system capable of supporting high speed.
					MOE-17	Mean corrective maintenance time ($M^{bar}ct$). (Blanchard 2011, 412)		
			FR-1.1	F-Hub shall collect health and status	MOE-4	Complete vs incomplete data collection.	SyR-44	The SWEF-Hub shall ensure 100% collection of transmitted data.
							SyR-5	The SWEF-Hub shall identify gaps in data transmitted 99% of the time.
			FR-1.3	The SWEF-Hub shall report health and status.	MOE-7	Number of status reports per number of data packages.	SyR-3	The SWEF-Hub shall be able to provide status and summarized reports on data being transmitted as well as data received/archived to system owners.
			FR-2.0	The SWEF-Hub shall collaborate with the fleet and secondary locations.	MOE-10	Percentage time of having real time collaboration.	SyR-43	SWEF-Hub shall have a communication system capable of supporting high speed.
			FR-3.0	The SWEF-Hub shall troubleshoot software and hardware.	MOE-16	Percentage of resolved issues.		
					MOE-17	Mean corrective maintenance time ($M^{bar}ct$). (Blanchard 2011, 412)		

Table 28. Level 2 Slice, Right Side of Map

St ID	Stakeholder	Description	MOP ID	Measures Of Performance (MOP)	TPM ID	Technical Performance Measures (TPMs)	Validation Criteria			
			NA	MOP not applicable	NA	TMP	A	D	I	T
St-5	NSWC PHD	Overall Command where facility will be located.	MOP-6	Number of intrusions per days.	TPM-8	Zero (0) security violations in fiscal year (FY).			X	
			MOP-13	Heat removal rate.	TPM-9	Maintain an hourly average temperature of 60 degrees Farenheit.	X			
			MOP-11	Frequency capacity.	TPM-10	Frequency capacity hourly averages.	X			
			MOP-5	Data transfer rate.	TPM-11	Consistent (hourly avg.) transmission rates greater or equal to 10 Gbps.	X			
			MOP-14	Percentage of data collected.	TPM-1	Percentage of lossed data packets < 1%.	X			
			MOP-3	Percentage Gap identification.	TPM-2	100% accountability of lossed data packets.	X			
			MOP-1	Number of status reports per number of data packages per day.	TPM-12	1:1 ratio of status received versus status reported.				X
			MOP-5	Data transfer rate.	TPM-11	Consistent (hourly avg.) transmission rates.	X			

Table 29. Level 3 Slice, Left Side of Map

St ID	Stakeholder	Description	PN ID	Primitive Needs (PN)	EN ID. Effective Needs (EN)	StR ID	Stakeholders Requirements (StR)
St-1	NSWC PHD Lead System Engineer	PHD Code 203	PN-2	Common solution that will provide technical capability across multiple systems across the Command.	7. Common processes across the combat system programs. 8. Technical collaboration of solutions and best practices.	SyR-19	The SWEF-Hub requirements shall be captured in overarching PHD Instructions.
						SyR-20	The SWEF-Hub personnel shall adhere to established NSWC PHD security processes and regulations for secured compartments.
						SyR-15	The SWEF-Hub personnel shall prepare technical changes for review, in order to ensure commonality and best practices are being used in existing and future labs.
St-4	A Department Manager	Air Dominance Department	PN-1	Combat System centric solution that will provide timely and ship board equivalent capability from SWEF-Hub.	19. Shipboard level combat system (CS) capability. 20. Shipboard level functionality (simulated and/or shipboard equivalent) to increase distance support and product development.	SyR-11	The SWEF-Hub shall be designed to provide shipboard equivalent systems capable of shipboard data to recreate issues.
St-2	L Department Manager	Littoral and Strike Warfare Department	PN-4	Infrastructure capable of providing timely technical support across department programs.	14. Shipboard level capability for programs. 15. Increase cyber capabilities for both red/blue team efforts. 16. Increase product development and refinement to increase technical competence for distance support efforts.		
St-6	S Department Manager	Ship Defense and Expeditionary Warfare Department	PN-4	Infrastructure capable of providing timely technical support across department programs.	14. Shipboard level capability for programs. 17. Increase directed energy technical capabilities. 18. Increase combat system integration and collaboration of common systems.		

Table 30. Level 3 Slice, Center of Map

St ID	Stakeholder	Description	FR ID / NFR ID	Functional Requirements (FRs) / Non-Functional Requirements (NFR)	MOE ID / NA	Measure Of Effectiveness (MOE) / MOE not applicable	SyR ID / NSyR ID	System Requirements (FSyR) / Non-System Requirements (NSyR) (Non-functionally related)
St-1	NSWC PHD Lead System Engineer	PHD Code 203	NFR-10	Compliance with building requirements and codes shall be an integral part of the SWEF-Hub.			NSyR-2	The SWEF-Hub shall be in compliance with SWEF building codes and requirements.
			NFR-7	Compliance with approved documentation shall be an integral part of the SWEF-Hub.			NSyR-4	The SWEF-Hub shall follow NSWC PHD Instructions for managing lab spaces and electronically tracking in and out personnel.
							NSyR-5	The SWEF-Hub shall follow Department processes for classified and unclassified data management, as applicable.
							NSyR-6	The SWEF-Hub shall adhere to Department processes for fleet distance support and interfacing with external entities.
			NFR-5	The stablishment of procedures and processes shall be part of the SWEF-Hub.			NSyR-1	The SWEF-Hub shall contain tailored processes for data storage duration and securing information being gathered from both, external and internal sources.
							NSyR-3	The SWEF-Hub shall contain tailored processes for data being exported to external and internal sources to include secure transfers and media types being used.
St-4	A Department Manager	Air Dominance Department	FR-1.2	The SWEF-Hub shall analyze and interpret data.	MOE-6	Percentage of processed data.	SyR-19	The SWEF-Hub shall load external shipboard data into its shipboard systems within eight hours.
							SyR-25	The SWEF-Hub shall load external shipboard data for analysis within eight hours.
St-2	L Department Manager	Littoral and Strike Warfare Department					SyR-26	The SWEF-Hub shall be able to load at a minimum two sets of external data for analysis.
							SyR-17	The SWEF-Hub shall be capable of software installations of shipboard systems within one hour period.
							SyR-20	SWEF-Hub shall have a high speed processor able to process at a minimum two sets of shipboard data at a given time.
St-6	S Department Manager	Ship Defense and Expeditionary Warfare Department					SyR-40	The SWEF-Hub shall have a simulation system to recreate issues.
							SyR-42	The SWEF-Hub shall analyze data from different combat systems.

Table 31. Level 3 Slice, Right Side of Map

St ID	Stakeholder	Description	MOP ID	Measures Of Performance (MOP)	TPM ID	Technical Performance Measures (TPMs)	Validation Criteria			
			NA	MOP not applicable	NA	TMP	A	D	I	T
St-1	NSWC PHD Lead System Engineer	PHD Code 203								
St-4	A Department Manager	Air Dominance Department	MOP-9	Data load-rate.	TPM-13	Number of objects transferred per second.				X
St-2	L Department Manager	Littoral and Strike Warfare Department	MOP-8	Software installation speed.	TPM-14	Upload/download/execute process total elapsed time > 59 minutes.				X
			MOP-2	Processor's speed.	TPM-15	Parallel/redundant channels with simultaneous processing speeds.	X			
St-6	S Department Manager	Ship Defense and Expeditionary Warfare Department								

Table 32. Level 4 Slice, Left Side of Map

St ID	Stakeholder	Description	PN ID	Primitive Needs (PN)	EN ID. Effective Needs (EN)	StR ID	Stakeholders Requirements (StR)
St-4	A Department Manager	Air Dominance Department	PN-1	Combat System centric solution that will provide timely and ship board equivalent capability from SWEF-Hub.	19. Shipboard level combat system (CS) capability. 20. Shipboard level functionality (simulated and/or shipboard equivalent) to increase distance support and product development.	SyR-12	The SWEF-Hub shall provide the capability needed to integrate cybersecurity capabilities for preventing, reporting, and exploiting vulnerabilities.
St-2	L Department Manager	Littoral and Strike Warfare Department	PN-4	Infrastructure capable of providing timely technical support across department programs.	14. Shipboard level capability for programs. 15. Increase cyber capabilities for both red/blue team efforts. 16. Increase product development and refinement to increase technical competence for distance support efforts.	SyR-13	SWEF-Hub shall provide the architecture for a seamless integration of both simulated and shipboard equivalent systems, integrated combat systems, shipboard networks, shipboard equivalent infrastructure, and elements at SWEF for current and future systems to improve distance support.
St-3	PHD Distance Support Customer Advocate	PHD Code 206	PN-3	Improve distance support response time and technology used to provide support.	9. Increase technical capability for distance support.		
St-6	S Department Manager	Ship Defense and Expeditionary Warfare Department	PN-4	Infrastructure capable of providing timely technical support across department programs.	14. Shipboard level capability for programs. 17. Increase directed energy technical capabilities. 18. Increase combat system integration and collaboration of common systems.	SyR-16	The SWEF-Hub shall provide the capability for integration of directed energy systems.

Table 33. Level 4 Slice, Center of Map

St ID	Stakeholder	Description	FR ID / NFR ID	Functional Requirements (FRs) / Non-Functional Requirements (NFR)	MOE ID / NA	Measure Of Effectiveness (MOE) / MOE not applicable	SyR ID / NSyR ID	System Requirements (FSyR) / Non-System Requirements (NSyR) (Non-functionally related)
St-4	A Department Manager	Air Dominance Department	FR-1.4	The SWEF-Hub shall implement cyber security.	MOE-8	Ratio of protected attacks to total attacks.	SyR-29	The SWEF-Hub shall have a cyber security system to provide continuous internal and external cyber defense capabilities.
							SyR-30	The SWEF-Hub shall utilize commercial software (COTS) for real time shipboard system monitoring.
							SyR-31	The SWEF-Hub shall use fiber optics and ethernet cable infrastructure to provide secured internet connectivity.
							SyR-32	The SWEF-Hub shall have an alert system to provide automated alerts when potential cyber threats are detected to internal SWEF-Hub managers and approved NSWC PHD personnel.
			NFR-7	Compliance with approved documentation shall be an integral part of the SWEF-Hub.			NSyR-8	SWEF-Hub shall be patched and maintained in accordance with the approved risk management framework (RMF) package.
			FR-1.4	The SWEF-Hub shall implement cyber security.	MOE-8	Ratio of protected attacks to total attacks.	SyR-12	The SWEF-Hub shall be able to identify supported and unsupported (gaps) platforms.
			NFR-1	Comparability with other systems shall be an integral part of the SWEF-Hub.			SyR-14	The SWEF-Hub shall utilize commercial products (COTs) for common data gathering, analyzing, and storing capabilities.
							SyR-22	The SWEF-Hub shall use commercial software (COT) to reduce the effort to operate shipboard baselines.
St-2	L Department Manager	Littoral and Strike Warfare Department					SyR-21	The SWEF-Hub shall use hardware capable of supporting different shipboard systems.
							SyR-23	The SWEF-Hub shall have a processor capable of processing different data formats coming from fleet platforms (e.g. cruisers, destroyers, LCSs, LPDs, carriers).
							SyR-16	The SWEF-Hub shall have an open system capable of being upgraded with minimal impact or downtime.
			NFR-2	Expandability shall be considered at the SWEF-Hub.			SyR-15	The SWEF-Hub architecture shall provide a extra 20% room for growth of hardware and software.
St-3	PHD Distance Support Customer Advocate	PHD Code 206	FR-1.0	The SWEF-Hub shall manage data.	MOE-4	Percent of managed data	SyR-28	The SWEF-Hub shall have a combat system baseline software within its environment.
			NFR-3	Reduncy shall be an integral part of the The SWEF-Hub.			SyR-38	The SWEF-Hub shall have redundant connection systems to provide redundant and secured connections to shipboard systems when providing distance support.
St-6	S Department Manager	Ship Defense and Expeditionary Warfare Department	NFR-4	Minimal ruggedization of systems shall be considered at the SWEF-Hub.			SyR-37	The SWEF-Hub shall provide the minimal shipboard ruggedized system hardware infrastructures.
			NFR-1	Comparability with other systems shall be an integral part of the SWEF-Hub.			NSyR-7	The SWEF-Hub shall identify how the physical infrastructure will be able to support future systems.
			NFR-1	Comparability with other systems shall be an integral part of the SWEF-Hub.			SyR-35	The SWEF-Hub shall have external interfaces for connections to laser weapon systems integration.
							SyR-36	The SWEF-Hub shall have a server infrastructure for external data coming from fielded laser systems.

Table 34. Level 4 Slice, Right Side of Map

St ID	Stakeholder	Description	MOP ID	Measures Of Performance (MOP)	TPM ID	Technical Performance Measures (TPMs)	Validation Criteria			
			NA	MOP not applicable	NA	TMP	A	D	I	T
St-4	A Department Manager	Air Dominance Department	MOP-10	Protected attacks per total attacks per day.	TPM-16	100% successful blockage of cyber treats.	X			
			MOP-11	Frequency capacity.	TPM-10	Frequency capacity hourly averages.	X			
			MOP-12	Ratio of identified/processed to reported threats.	TPM-17	1:1 ratio of threats identified versus threats reported.				X
St-2	L Department Manager	Littoral and Strike Warfare Department	MOP-7	Upgrade downtime.	TPM-18	Upgrade downtime no greater then 48 hours.	X			
St-3	PHD Distance Support Customer Advocate	PHD Code 206								
St-6	S Department Manager	Ship Defense and Expeditionary Warfare Department								

APPENDIX B. ALLOCATION MATRIXES

The architecture and design are related by the idea that the architecture describes how a system should be structured while the design ensures that the architecture is achievable and capable of performing within the limits of the requirements. The architecture's structured actions are related to the design's physical elements due to the reasonable presumption that the physical elements will enable the action. (INCOSE 2015).

The system elements (physical elements: computer, antenna, software, etc.) are the parts of the architectural entities (models, views, viewpoints, diagrams, etc.). Allocation matrices are created to show the relationship between the elements of different architectural entities. For example, an allocation matrix will show the relationships of a functional flow-block diagram to a physical block diagram. The allocation matrices, Tables 35 to 50 show the relationship between the elements of functional entities vs the element of the physical entity. Each entity has a different functionality; however, some of the elements are the same or similar. In these matrices the "X" shows that a functional element is related to the corresponding physical element. These allocation matrices show that at least one physical element matches one functional element and vice versa (INCOSE 2015). The first set are the near-term allocation matrices and the second set are the long-term allocation matrices.

Table 35. CBM Near-Term

	A.1.1 Antenna	A.1.2 Router	A.1.3 Transmitter	A.1.4 Receiver	A.2.0 Help Desk	A.2.1 Telephone	A.2.2 Personnel	A.2.3 Computer	A.2.3.1 Software	A.2.3.1.1 Operating System	A.2.3.1.2 Outlook	A.2.3.1.3 Database Management	A.2.3.1.4 Combat System Software	A.2.3.1.5 Cyber Security Software	A.2.3.2 Hardware	A.2.3.2.1 Display Monitors	A.2.3.2.2 Mother Board	A.2.3.2.2.1 Processor	A.2.3.2.2.2 Graphics Card	A.2.3.2.2.3 Network Ident. Card	A.2.3.2.2.4 Solid State Drive	A.2.3.2.2.5 RAM	A.2.3.2.3 Power Supply	A.3.0 Power Generator	A.4.0 HVAC System	A.5.0 Biometric Security System
2.1 Scheduled Maintenance Performed	N/A																									
2.2 Transmit NOC Data to SWEF-HUB	X	X	X											X												
1.1 Stationed Monitoring	X	X	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X
2.3 Receive NOC	X	X	X	X			X	X	X	X	X	X		X	X	X	X	X	X	X	X	X				
2.4 Identify Tech Center					X		X	X	X	X		X			X	X	X	X	X	X	X	X				
2.5 Transmit NOC to Tech Center	X	X	X		X		X	X	X	X	X	X		X	X	X	X	X	X	X	X	X				
2.6 Receive NOC from SWEF-HUB	X	X		X				X	X	X	X	X	N/A	X	X	X	X	X	X	X	X	X				
2.7 Analyze NOC Data								X	X	X		X		X	X	X	X	X	X	X	X	X				
2.8 Transmit COA to SWEF-HUB	X	X	X				X			X	X			X	X	X	X	X	X	X	X	X				
2.9 Receive COA from Tech Center	X	X		X	X		X	X	X	X	X	X		X	X	X	X	X	X	X	X	X				
2.10 Identify Ship Element								X	X	X	X	X				X	X	X	X	X	X	X				
2.11 Transmit COA to Ship Element	X	X	X		X		X	X	X	X	X	X		X		X	X	X	X	X	X	X				

Table 36. CBM Near-Term (cont.)

	A.1.1 Antenna	A.1.2 Router	A.1.3 Transmitter	A.1.4 Receiver	A.2.0 Help Desk	A.2.1 Telephone	A.2.2 Personnel	A.2.3 Computer	A.2.3.1 Software	A.2.3.1.1 Operating System	A.2.3.1.2 Outlook	A.2.3.1.3 Database Management	A.2.3.1.4 Combat System Software	A.2.3.1.5 Cyber Security Software	A.2.3.2 Hardware	A.2.3.2.1 Display Monitors	A.2.3.2.2 Mother Board	A.2.3.2.2.1 Processor	A.2.3.2.2.2 Graphics Card	A.2.3.2.2.3 Network Ident. Card	A.2.3.2.2.4 Solid State Drive	A.2.3.2.2.5 RAM	A.2.3.2.3 Power Supply	A.3.0 Power Generator	A.4.0 HVAC System	A.5.0 Biometric Security System
2.12 Receive COA from SWEF-HUB	N/A																									
2.13 Implement COA																										
2.14 Complete COA																										
2.15 Transmit COA NOC to SWEF-HUB																										
2.16 Receive COA NOC	X	X		X			X			X	X	X	N/A	X	X	X	X	X	X	X	X	X	X			
2.17 Transmit COA NOC to Tech Center	X	X	X				X			X	X	X		X	X	X	X	X	X	X	X	X	X			
2.18 Receive COA NOC from SWEF-HUB	X	X		X			X			X	X	X		X	X	X	X	X	X	X	X	X	X			
2.19 Closeout Issue															X	X	X	X	X	X	X	X	X			
2.20 Transmit Message of Issue Closeout	X	X	X				X			X	X	X		X	X	X	X	X	X	X	X	X	X			
2.21 Receive Closeout Issue Message	X	X		X			X			X	X	X		X		X	X	X	X	X	X	X	X			
1.7 Store Data		X	X	X			X			X	X	X		X		X	X	X	X	X	X	X	X			

Table 37. Raw Data Collection Near-Term

	A.1.1 Antenna	A.1.2 Router	A.1.3 Transmitter	A.1.4 Receiver	A.2.0 Help Desk	A.2.1 Telephone	A.2.2 Personnel	A.2.3 Computer	A.2.3.1 Software	A.2.3.1.1 Operating System	A.2.3.1.2 Outlook	A.2.3.1.3 Database Management	A.2.3.1.4 Combat System Software	A.2.3.1.5 Cyber Security Software	A.2.3.2 Hardware	A.2.3.2.1 Display Monitors	A.2.3.2.2 Mother Board	A.2.3.2.2.1 Processor	A.2.3.2.2.2 Graphics Card	A.2.3.2.2.3 Network Ident. Card	A.2.3.2.2.4 Solid State Drive	A.2.3.2.2.5 RAM	A.2.3.2.3 Power Supply	A.3.0 Power Generator	A.4.0 HVAC System	A.5.0 Biometric Security System
2.1 Scheduled Maintenance Performed	N/A																									
2.2 Transmit NOC Data to SWEF-HUB	X	X	X										N/A	X												
1.1 Stationed Monitoring	X	X	X	X	X	X	X	X	X	X	X	X				X	X	X	X	X	X	X	X	X	X	X
2.3 Receive NOC	X	X		X			X			X	X	X		X		X	X	X	X	X	X	X				
3.4 Review Data							X			X		X		X		X	X	X	X	X	X	X				
1.6 Catagorize Data							X			X		X		X		X	X	X	X	X	X	X				
1.7 Store Data		X	X	X			X			X		X		X		X	X	X	X	X	X	X				

Table 38. Troubleshoot Near-Term

	A.1.1 Antenna	A.1.2 Router	A.1.3 Transmitter	A.1.4 Receiver	A.2.0 Help Desk	A.2.1 Telephone	A.2.2 Personnel	A.2.3 Computer	A.2.3.1 Software	A.2.3.1.1 Operating System	A.2.3.1.2 Outlook	A.2.3.1.3 Database Management	A.2.3.1.4 Combat System Software	A.2.3.1.5 Cyber Security Software	A.2.3.2 Hardware	A.2.3.2.1 Display Monitors	A.2.3.2.2 Mother Board	A.2.3.2.2.1 Processor	A.2.3.2.2.2 Graphics Card	A.2.3.2.2.3 Network Ident. Card	A.2.3.2.2.4 Solid State Drive	A.2.3.2.2.5 RAM	A.2.3.2.3 Power Supply	A.3.0 Power Generator	A.4.0 HVAC System	A.5.0 Biometric Security System
4.1 System issue detected by ship force	N/A																									
4.2 Transmit secured email	X	X	X											X												
1.1 Stationed Monitoring	X	X	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X
4.3 Receive Secured Email	X	X		X	X		X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X			
4.4 Analyze Data for sorting							X			X		X				X	X	X	X	X	X	X	X			
2.4 Identify Tech Center					X		X	X	X	X		X			X	X	X	X	X	X	X	X	X			
4.5 Receive notification	X	X	X		X		X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X			
4.6 Analyze Data for Anomalies					X			X	X	X		X			X	X	X	X	X	X	X	X	X	X			
4.7 Troubleshoot Issue								X	X	X		X			X	X	X	X	X	X	X	X	X	X			
4.8 Develop Solution								X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X			
4.9 Receive Secured Email w/ Solution	X	X		X			X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X			
4.10 Receive Secured Email w/ Solution from SWEF-HUB	X	X	X				X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X			

Table 39. Troubleshoot Near-Term (cont.)

	A.1.1 Antenna	A.1.2 Router	A.1.3 Transmitter	A.1.4 Receiver	A.2.0 Help Desk	A.2.1 Telephone	A.2.2 Personnel	A.2.3 Computer	A.2.3.1 Software	A.2.3.1.1 Operating System	A.2.3.1.2 Outlook	A.2.3.1.3 Database Management	A.2.3.1.4 Combat System Software	A.2.3.1.5 Cyber Security Software	A.2.3.2 Hardware	A.2.3.2.1 Display Monitors	A.2.3.2.2 Mother Board	A.2.3.2.2.1 Processor	A.2.3.2.2.2 Graphics Card	A.2.3.2.2.3 Network Ident. Card	A.2.3.2.2.4 Solid State Drive	A.2.3.2.2.5 RAM	A.2.3.2.3 Power Supply	A.3.0 Power Generator	A.4.0 HVAC System	A.5.0 Biometric Security System
4.11 Implement Solution	N/A																									
4.12 Issue Resolved?																										
4.13 Troubleshoot Continuation																										
4.14 Develop Notification of Completion (NOC)																										
2.3 Receive NOC	X	X		X			X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X			
2.4 Identify Tech Center		X					X	X	X	X		X			X	X	X	X	X	X	X	X	X			
4.15 Receive notification of update	X	X	X				X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X			
4.16 Review NOC								X	X	X		X		X	X	X	X	X	X	X	X	X	X			
2.19 Closeout Issue								X	X	X		X		X	X	X	X	X	X	X	X	X	X			
2.20 Transmit Message of Issue Closeout	X	X	X				X			X	X	X		X		X	X	X	X	X	X	X	X			
2.21 Receive Closeout Issue Message	X	X		X			X			X	X	X		X		X	X	X	X	X	X	X	X			
1.7 Store Data		X	X	X			X			X		X		X		X	X	X	X	X	X	X	X			

Table 40. Secondary Collaboration

	A.1.1 Antenna	A.1.2 Router	A.1.3 Transmitter	A.1.4 Receiver	A.2.0 Help Desk	A.2.1 Telephone	A.2.2 Personnel	A.2.3 Computer	A.2.3.1 Software	A.2.3.1.1 Operating System	A.2.3.1.2 Outlook	A.2.3.1.3 Database Management	A.2.3.1.4 Combat System Software	A.2.3.1.5 Cyber Security Software	A.2.3.2 Hardware	A.2.3.2.1 Display Monitors	A.2.3.2.2 Mother Board	A.2.3.2.2.1 Processor	A.2.3.2.2.2 Graphics Card	A.2.3.2.2.3 Network Ident. Card	A.2.3.2.2.4 Solid State Drive	A.2.3.2.2.5 RAM	A.2.3.2.3 Power Supply	A.3.0 Power Generator	A.4.0 HVAC System	A.5.0 Biometric Security System
6.1 Request Use of Facility	N/A																									
1.1 Stationed Monitoring	X	X	X	X		X	X	X		X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X
6.2 Receive Request	X	X		X			X			X	X	X		X		X	X	X	X	X	X	X	X			
6.3 Process Request							X			X	X	X		X		X	X	X	X	X	X	X	X			
6.4 Identify Tech Center							X			X	X	X				X	X	X	X	X	X	X	X			
6.5 Forward Request to Tech Center	X	X	X				X			X	X	X		X		X	X	X	X	X	X	X	X			
6.6 Receive Request from SWEF-HUB	X	X		X			X			X	X	X		X		X	X	X	X	X	X	X	X			
6.7 Approve Request										X		X		X		X	X	X	X	X	X	X	X			
6.8 Send Approval to SWEF-HUB	X	X	X							X	X	X		X		X	X	X	X	X	X	X	X			
6.9 Receive Approval	X	X		X			X			X	X	X		X		X	X	X	X	X	X	X	X			
6.10 Send Approval to System Element	X	X	X				X			X	X	X		X		X	X	X	X	X	X	X	X			

Table 41. Secondary Collaboration (cont.)

	A.1.1 Antenna	A.1.2 Router	A.1.3 Transmitter	A.1.4 Receiver	A.2.0 Help Desk	A.2.1 Telephone	A.2.2 Personnel	A.2.3 Computer	A.2.3.1 Software	A.2.3.1.1 Operating System	A.2.3.1.2 Outlook	A.2.3.1.3 Database Management	A.2.3.1.4 Combat System Software	A.2.3.1.5 Cyber Security Software	A.2.3.2 Hardware	A.2.3.2.1 Display Monitors	A.2.3.2.2 Mother Board	A.2.3.2.2.1 Processor	A.2.3.2.2.2 Graphics Card	A.2.3.2.2.3 Network Ident. Card	A.2.3.2.2.4 Solid State Drive	A.2.3.2.2.5 RAM	A.2.3.2.3 Power Supply	A.3.0 Power Generator	A.4.0 HVAC System	A.5.0 Biometric Security System
6.11 Receive Approval	N/A																									
6.12 Send Data needed for Simulated Testing																										
6.13 Go to SWEF-HUB to Setup System										X	X	X		X		X	X	X	X	X	X	X	X	X		X
6.14 Prepare SWEF-HUB for Simulated Test Environment										X	X	X	X	X		X	X	X	X	X	X	X	X	X		
6.15 Receive Data	X	X	X							X	X	X	X	X		X	X	X	X	X	X	X	X	X		
6.16 Implement Data into Simulated Test Environment	X	X		X			X			X	X	X	X	X		X	X	X	X	X	X	X	X	X		
6.17 Run Simulation		X	X				X			X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X
6.18 Recorded Results										X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	
1.7 Store Data		X	X	X						X	X	X	X	X		X	X	X	X	X	X	X	X			
6.19 Send Results to System Element	X	X	X							X	X	X		X		X	X	X	X	X	X	X	X			
6.20 Received Results	X	X		X						X	X	X		X		X	X	X	X	X	X	X	X			

Table 42. CBM Long-Term

	B.1.1 Antenna	B.1.2 Router	B.1.3 Transmitter	B.1.4 Receiver	B.2.0 Help Desk	B.2.1 Telephone	B.2.2 Personnel	B.2.3 Computer	B.2.3.1 Software	B.2.3.1.1 Operating System	B.2.3.1.2 Machine Learning	B.2.3.1.2.1 Database Management	B.2.3.1.3 Outlook	B.2.3.1.4 Combat System Software	B.2.3.1.5 Cyber Security System	B.2.3.2 Hardware	B.2.3.2.1 Display Monitors	B.2.3.2.2 Mother Board	B.2.3.2.2.1 Processor	B.2.3.2.2.2 Graphics Card	B.2.3.2.2.3 Network Ident. Card	B.2.3.2.2.4 Solid State Drive	B.2.3.2.2.5 RAM	B.2.3.2.3 Power Supply	B.2.3.2.4 Webcam	B.2.3.2.5 Speakers	B.3.0 Power Generator	B.4.0 HVAC System	B.5.0 Biometric Security System
2.1 Scheduled Maintenance Performed	N/A																												
2.2 Transmit NOC Data to SWEF-HUB	X	X	X																										
1.1 Stationed Monitoring	X	X	X	X		X	X			X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
2.3 Receive NOC	X	X		X						X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X			
7.7 Automated Storage of Data		X	X	X						X	X	X			X	X	X	X	X	X	X	X	X	X	X	X			
8.1 Automated Analysis of NOC Data		X	X	X						X	X	X			X	X	X	X	X	X	X	X	X	X	X	X			
8.2 Identify Appropriate Tech Center		X	X	X						X	X	X			X	X	X	X	X	X	X	X	X	X	X	X			
8.3 Transmit Message to SWEF-HUB Personnel	X	X	X							X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X			
8.4 Analyze Message for Accuracy	X	X		X			X			X		X	X		X	X	X	X	X	X	X	X	X	X	X	X			
8.5 Transmit Message to Tech Center	X	X	X				X			X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X			
8.6 Receive Message	X	X		X						X		X	X		X	X	X	X	X	X	X	X	X	X	X	X			

Table 43. CBM Long-Term (cont.)

	B.1.1 Antenna	B.1.2 Router	B.1.3 Transmitter	B.1.4 Receiver	B.2.0 Help Desk	B.2.1 Telephone	B.2.2 Personnel	B.2.3 Computer	B.2.3.1 Software	B.2.3.1.1 Operating System	B.2.3.1.2 Machine Learning	B.2.3.1.2.1 Database Management	B.2.3.1.3 Outlook	B.2.3.1.4 Combat System Software	B.2.3.1.5 Cyber Security System	B.2.3.2 Hardware	B.2.3.2.1 Display Monitors	B.2.3.2.2 Mother Board	B.2.3.2.2.1 Processor	B.2.3.2.2.2 Graphics Card	B.2.3.2.2.3 Network Ident. Card	B.2.3.2.2.4 Solid State Drive	B.2.3.2.2.5 RAM	B.2.3.2.3 Power Supply	B.2.3.2.4 Webcam	B.2.3.2.5 Speakers	B.3.0 Power Generator	B.4.0 HVAC System	B.5.0 Biometric Security System
8.7 Analyze COA Determined by ML Program										X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X			
8.8 Approve COA										X		X			X	X	X	X	X	X	X	X	X	X	X	X	X			
8.9 Transmit COA to SWEF-HUB	X	X	X							X		X	X		X	X	X	X	X	X	X	X	X	X	X	X	X			
8.10 Input Data into ML Program							X			X	X	X			X	X	X	X	X	X	X	X	X	X	X	X	X			
8.11 Receive Inputted Data	X	X		X						X	X	X			X	X	X	X	X	X	X	X	X	X	X	X	X			
8.12 Analyze Data										X	X	X			X	X	X	X	X	X	X	X	X	X	X	X	X			
8.13 Identify Ship Element										X	X	X			X	X	X	X	X	X	X	X	X	X	X	X	X			
8.14 Transmit COA Message	X	X	X							X	X	X			X	X	X	X	X	X	X	X	X	X	X	X	X			
8.15 Receive COA	N/A																													
8.16 Implement COA																														
8.17 Complete COA																														
8.18 Transmit COA NOC to SWEF-HUB																														

Table 44. CBM Long-Term (cont.)

	B.1.1 Antenna	B.1.2 Router	B.1.3 Transmitter	B.1.4 Receiver	B.2.0 Help Desk	B.2.1 Telephone	B.2.2 Personnel	B.2.3 Computer	B.2.3.1 Software	B.2.3.1.1 Operating System	B.2.3.1.2 Machine Learning	B.2.3.1.2.1 Database Management	B.2.3.1.3 Outlook	B.2.3.1.4 Combat System Software	B.2.3.1.5 Cyber Security System	B.2.3.2 Hardware	B.2.3.2.1 Display Monitors	B.2.3.2.2 Mother Board	B.2.3.2.2.1 Processor	B.2.3.2.2.2 Graphics Card	B.2.3.2.2.3 Network Ident. Card	B.2.3.2.2.4 Solid State Drive	B.2.3.2.2.5 RAM	B.2.3.2.3 Power Supply	B.2.3.2.4 Webcam	B.2.3.2.5 Speakers	B.3.0 Power Generator	B.4.0 HVAC System	B.5.0 Biometric Security System
8.19 Receive COA NOC	X	X		X						X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X			
7.7 Automated Storage of Data		X	X	X						X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X			
8.20 Transmit Confirmation Message for Delivery	X	X	X							X	X	X			X	X	X	X	X	X	X	X	X	X	X	X			
8.21 Confirm Message Delivery							X			X			X		X	X	X	X	X	X	X	X	X	X	X	X			
8.22 Receive COA NOC from SWEF-HUB	X	X		X						X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X			
2.19 Closeout Issue										X		X			X	X	X	X	X	X	X	X	X	X	X	X			
2.20 Transmit Message of Issue Closeout	X	X	X							X		X	X		X	X	X	X	X	X	X	X	X	X	X	X			
2.21 Receive Closeout Issue Message	X	X		X						X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X			
7.7 Automated Storage of Data		X	X	X						X	X	X			X	X	X	X	X	X	X	X	X	X	X	X			

Table 45. Raw Data Collection Long-Term

	B.1.1 Antenna	B.1.2 Router	B.1.3 Transmitter	B.1.4 Receiver	B.2.0 Help Desk	B.2.1 Telephone	B.2.2 Personnel	B.2.3 Computer	B.2.3.1 Software	B.2.3.1.1 Operating System	B.2.3.1.2 Machine Learning	B.2.3.1.2.1 Database Management	B.2.3.1.3 Outlook	B.2.3.1.4 Combat System Software	B.2.3.1.5 Cyber Security System	B.2.3.2 Hardware	B.2.3.2.1 Display Monitors	B.2.3.2.2 Mother Board	B.2.3.2.2.1 Processor	B.2.3.2.2.2 Graphics Card	B.2.3.2.2.3 Network Ident. Card	B.2.3.2.2.4 Solid State Drive	B.2.3.2.2.5 RAM	B.2.3.2.3 Power Supply	B.2.3.2.4 Webcam	B.2.3.2.5 Speakers	B.3.0 Power Generator	B.4.0 HVAC System	B.5.0 Biometric Security System
2.1 Scheduled Maintenance Performed	N/A																												
7.2 Automated Securing of Data		X	X	X						X	X	X	X		X		X	X	X	X	X	X	X	X	X	X			
7.3 Automated Transition of Secured Data to SWEF-HUB	X	X		X						X	X	X	X		X		X	X	X	X	X	X	X	X	X	X			
1.1 Stationed Monitoring	X	X	X	X		X	X			X	X	X	X		X		X	X	X	X	X	X	X	X	X	X	X	X	X
7.4 Receive Secured Data	X	X		X						X	X	X	X		X		X	X	X	X	X	X	X	X	X	X			
7.5 Analyze Database for Categorization		X								X	X	X			X		X	X	X	X	X	X	X	X	X	X			
7.6 Automated Categorization of Data		X								X	X	X			X		X	X	X	X	X	X	X	X	X	X			
9.1 Send Notification of Categorized Data to Monitored for confirmation	X	X	X							X	X	X	X	N/A	X		X	X	X	X	X	X	X	X	X	X			
9.2 Received Confirmation Notification	X	X		X			X			X		X	X		X		X	X	X	X	X	X	X	X	X	X			
9.3 Confirm Categorization							X			X		X			X		X	X	X	X	X	X	X	X	X	X			
9.4 Send Confirmation	X	X	X				X			X		X	X		X		X	X	X	X	X	X	X	X	X	X			
9.5 Receive Confirmation	X	X		X						X	X	X	X		X		X	X	X	X	X	X	X	X	X	X			
9.6 ML Program logs and records decision for future use		X	X	X						X	X	X	X		X		X	X	X	X	X	X	X	X	X	X			
7.7 Automated Storage of Data		X	X	X						X	X	X			X		X	X	X	X	X	X	X	X	X	X			

Table 46. Troubleshooting Long-Term

	B.1.1 Antenna	B.1.2 Router	B.1.3 Transmitter	B.1.4 Receiver	B.2.0 Help Desk	B.2.1 Telephone	B.2.2 Personnel	B.2.3 Computer	B.2.3.1 Software	B.2.3.1.1 Operating System	B.2.3.1.2 Machine Learning	B.2.3.1.2.1 Database Management	B.2.3.1.3 Outlook	B.2.3.1.4 Combat System Software	B.2.3.1.5 Cyber Security System	B.2.3.2 Hardware	B.2.3.2.1 Display Monitors	B.2.3.2.2 Mother Board	B.2.3.2.2.1 Processor	B.2.3.2.2.2 Graphics Card	B.2.3.2.2.3 Network Ident. Card	B.2.3.2.2.4 Solid State Drive	B.2.3.2.2.5 RAM	B.2.3.2.3 Power Supply	B.2.3.2.4 Webcam	B.2.3.2.5 Speakers	B.3.0 Power Generator	B.4.0 HVAC System	B.5.0 Biometric Security System
7.1 Automated Scheduled Data Pull	X	X	X					X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X					
7.2 Automated Securing of Data	X	X		X				X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X					
7.3 Automated Transition of Secured Data to SWEF-HUB	X	X	X							X	X	X	X		X		X	X	X	X	X	X	X	X					
1.1 Stationed Monitoring	X	X	X	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
7.4 Receive Secured Data	X	X		X	X			X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X			
10.1 Analyze Data for Anomalies		X	X	X				X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X			
10.2 Anomaly detected								X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X			
10.3 Analyze database to determine issue		X	X	X				X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X			
10.4 Issue Identified								X	X	X	X	X	X	N/A	X	X	X	X	X	X	X	X	X	X	X	X			
10.5 Analyze Database for solution		X	X	X				X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X			
8.2 Identify Appropriate Tech Center		X	X	X				X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X			
10.6 Ensure appropriate personnel is notified		X	X				X			X		X	X		X		X	X	X	X	X	X	X	X	X	X			
10.7 Receive notification		X		X			X			X		X	X		X		X	X	X	X	X	X	X	X	X	X			
10.8 Access SWEF-HUB database	X	X								X		X	X		X		X	X	X	X	X	X	X	X	X	X			

Table 47. Troubleshooting Long-Term (cont.)

	B.1.1 Antenna	B.1.2 Router	B.1.3 Transmitter	B.1.4 Receiver	B.2.0 Help Desk	B.2.1 Telephone	B.2.2 Personnel	B.2.3 Computer	B.2.3.1 Software	B.2.3.1.1 Operating System	B.2.3.1.2 Machine Learning	B.2.3.1.2.1 Database Management	B.2.3.1.3 Outlook	B.2.3.1.4 Combat System Software	B.2.3.1.5 Cyber Security System	B.2.3.2 Hardware	B.2.3.2.1 Display Monitors	B.2.3.2.2 Mother Board	B.2.3.2.2.1 Processor	B.2.3.2.2 Graphics Card	B.2.3.2.2.3 Network Ident. Card	B.2.3.2.2.4 Solid State Drive	B.2.3.2.2.5 RAM	B.2.3.2.3 Power Supply	B.2.3.2.4 Webcam	B.2.3.2.5 Speakers	B.3.0 Power Generator	B.4.0 HVAC System	B.5.0 Biometric Security System
10.9 Review Solution Provided	X	X		X						X		X	X		X		X	X	X	X	X	X	X	X	X	X			
10.10 Receive confirmation or solution	X	X		X			X			X		X	X		X		X	X	X	X	X	X	X	X					
4.10 Receive Secured Email w/ Solution from SWEF-HUB	X	X	X				X			X		X	X		X		X	X	X	X	X	X	X	X					
4.11 Implement Solution	N/A																												
4.12 Issue Resolved?																													
4.13 Troubleshoot Continuation																													
4.14 Develop Notification of Completion (NOC)	X	X	X											N/A															
10.11 Receive NOC from Ship Element	X	X		X						X	X	X	X		X		X	X	X	X	X	X	X	X					
2.4 Identify Tech Center		X	X	X						X	X	X			X		X	X	X	X	X	X	X	X					
10.12 Send "Closeout Issue" message	X	X	X							X	X	X	X		X		X	X	X	X	X	X	X	X					
10.13 Receive Notification from SWEF-HUB	X	X		X						X	X	X	X		X		X	X	X	X	X	X	X	X					
4.16 Review NOC										X		X	X		X		X	X	X	X	X	X	X	X					
10.14 Accept Closeout Issue message	X	X	X							X		X	X		X		X	X	X	X	X	X	X	X					
2.19 Closeout Issue	X	X		X						X	X		X		X		X	X	X	X	X	X	X	X					
7.7 Automated Storage of Data															X		X	X	X	X	X	X	X	X					

Table 48. Secondary Collaboration Long-Term

	B.1.1 Antenna	B.1.2 Router	B.1.3 Transmitter	B.1.4 Receiver	B.2.0 Help Desk	B.2.1 Telephone	B.2.2 Personnel	B.2.3 Computer	B.2.3.1 Software	B.2.3.1.1 Operating System	B.2.3.1.2 Machine Learning	B.2.3.1.2.1 Database Management	B.2.3.1.3 Outlook	B.2.3.1.4 Combat System Software	B.2.3.1.5 Cyber Security System	B.2.3.2 Hardware	B.2.3.2.1 Display Monitors	B.2.3.2.2 Mother Board	B.2.3.2.2.1 Processor	B.2.3.2.2.2 Graphics Card	B.2.3.2.2.3 Network Ident. Card	B.2.3.2.2.4 Solid State Drive	B.2.3.2.2.5 RAM	B.2.3.2.3 Power Supply	B.2.3.2.4 Webcam	B.2.3.2.5 Speakers	B.3.0 Power Generator	B.4.0 HVAC System	B.5.0 Biometric Security System
6.1 Request Use of Facility	X	X	X										X																
1.1 Stationed Monitoring	X	X	X	X		X	X			X	X	X	X		X		X	X	X	X	X	X	X	X	X	X	X	X	X
6.2 Receive Request	X	X		X						X	X	X	X		X		X	X	X	X	X	X	X	X	X	X			
12.1 Access Database to Process Request	X	X	X	X						X	X	X	X		X		X	X	X	X	X	X	X	X	X	X			
12.2 Access Database to Identify Tech Center	X	X	X	X						X	X	X	X		X		X	X	X	X	X	X	X	X	X	X			
12.3 Transmit Message Prompt to Help Desk Personnel for Confirmation	X	X	X							X	X	X	X		X		X	X	X	X	X	X	X	X	X	X			
12.4 Receive Message Prompt to Confirm Forwarding of Request	X	X		X			X			X		X	X		X		X	X	X	X	X	X	X	X	X	X			
12.5 Analyze Data							X			X		X	X		X		X	X	X	X	X	X	X	X	X	X			
12.6 Confirm Forwarding of Request															X		X	X	X	X	X	X	X	X	X	X			
6.6 Receive Request from SWEF-HUB	X	X		X						X	X	X	X		X		X	X	X	X	X	X	X	X	X	X			
6.7 Approve Request										X		X	X		X		X	X	X	X	X	X	X	X	X	X			
6.8 Send Approval to SWEF-HUB	X	X	X							X		X	X		X		X	X	X	X	X	X	X	X	X	X			
6.9 Receive Approval	X	X		X						X	X	X	X		X		X	X	X	X	X	X	X	X	X	X			

Table 49. Secondary Collaboration Long-Term (cont.)

	B.1.1 Antenna	B.1.2 Router	B.1.3 Transmitter	B.1.4 Receiver	B.2.0 Help Desk	B.2.1 Telephone	B.2.2 Personnel	B.2.3 Computer	B.2.3.1 Software	B.2.3.1.1 Operating System	B.2.3.1.2 Machine Learning	B.2.3.1.2.1 Database Management	B.2.3.1.3 Outlook	B.2.3.1.4 Combat System Software	B.2.3.1.5 Cyber Security System	B.2.3.2 Hardware	B.2.3.2.1 Display Monitors	B.2.3.2.2 Mother Board	B.2.3.2.2.1 Processor	B.2.3.2.2.2 Graphics Card	B.2.3.2.2.3 Network Ident. Card	B.2.3.2.2.4 Solid State Drive	B.2.3.2.2.5 RAM	B.2.3.2.3 Power Supply	B.2.3.2.4 Webcam	B.2.3.2.5 Speakers	B.3.0 Power Generator	B.4.0 HVAC System	B.5.0 Biometric Security System
12.7 Access Database to Identify System Element															X		X	X	X	X	X	X	X	X	X	X			
12.8 Identify System Element		X	X	X											X		X	X	X	X	X	X	X	X	X	X			
12.9 Transmit Approval Message to System Element	X	X	X							X	X	X	X																
6.11 Receive Approval	N/A																												
6.12 Send Data needed for Simulated Testing																													
6.13 Go to SWEF-HUB to Setup System										X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X			X
6.14 Prepare SWEF-HUB for Simulated Test Environment										X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
12.10 Implement ML Program to Test System	X	X		X						X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X			
12.11 Assimilate Test System										X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
6.15 Receive Data	X	X		X						X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X			
12.12 Implement Data into System		X	X							X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X			

Table 50. Secondary Collaboration Long-Term (cont.)

	B.1.1 Antenna	B.1.2 Router	B.1.3 Transmitter	B.1.4 Receiver	B.2.0 Help Desk	B.2.1 Telephone	B.2.2 Personnel	B.2.3 Computer	B.2.3.1 Software	B.2.3.1.1 Operating System	B.2.3.1.2 Machine Learning	B.2.3.1.2.1 Database Management	B.2.3.1.3 Outlook	B.2.3.1.4 Combat System Software	B.2.3.1.5 Cyber Security System	B.2.3.2 Hardware	B.2.3.2.1 Display Monitors	B.2.3.2.2 Mother Board	B.2.3.2.2.1 Processor	B.2.3.2.2.2 Graphics Card	B.2.3.2.2.3 Network Ident. Card	B.2.3.2.2.4 Solid State Drive	B.2.3.2.2.5 RAM	B.2.3.2.3 Power Supply	B.2.3.2.4 Webcam	B.2.3.2.5 Speakers	B.3.0 Power Generator	B.4.0 HVAC System	B.5.0 Biometric Security System
12.13 Transmit Message Prompt to Begin Test		X	X							X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X			
12.14 Receive Message		X		X						X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X			
12.15 Confirm to Begin Test		X	X							X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X			
12.16 Receive Confirmation		X		X						X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X			
6.17 Run Simulation										X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X			
6.18 Record Results										X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X			
7.7 Automated Storage of Data		X	X	X						X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X			
12.17 Review Test Results										X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X			
12.18 Send Command to Forward Test Results		X	X							X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X			
12.19 Receive Command		X		X						X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X			
12.20 Forward Test Result to System Element	X	X	X							X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X			
6.20 Received Results	N/A																												

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Amazon. n.d. “Corrugated Boxes.” Accessed November 8, 2019. https://www.amazon.com/Boxes-Fast-BF14106-Cardboard-Corrugated/dp/B077BWX7VY.

ArchiMate. n.d. “Architecture Viewpoints.” Accessed September 26, 2019. https://pubs.opengroup.org/architecture/archimate-doc/ts_archimate/chap9.html.

Baslisle, Phillip M. 2011. *Fleet Readiness Review Panel Report.* Norfolk, VA: U.S. Fleet Forces Command. http://www.scribd.com/doc/43245136/Baslisle-Report-on-FRP-of-Surface-Force-Readiness.

Blanchard, Benjamin S., and Wolter J. Fabrycky. 2011. *Systems Engineering and Analysis. 5th ed.* 1 Lake Street, Upper Saddle River, NJ: Prentice Hall.

Buede, Dennis M. 2016. *The Engineering Design of Systems: Models and Methods*, 2nd Ed. Hoboken, NJ: John Wiley & Sons.

Buy Mars. n.d. “Planet Earth.” Accessed November 7, 2019. http://www.buymars.com/planet-earth.

Department of the Navy. 2017. *Cybersecurity Program.* NSWC PHD INST 5239.2. Port Hueneme, CA: Department of the Navy.

Department of Defense. 2017. *Operation of the Defense Acquisition System.* DOD Directive 5000.02. Washington, DC: Department of Defense.

Dodcio. 2010. “DODAF-DOD Architecture Framework Version 2.02 – DOD Deputy Chief Information Officer.” September 30, 2010. http://dodcio.defense.gov/Library/Dod-Architecture-Framework/dodaf20_viewpoints/.

GDPR Informer. 2017. “6 Essential Data Protection Methods.” October 6, 2017. https://gdprinformer.com/gdpr-articles/6-essential-data-protection-methods.

Harney, Robert C. 2011. *Combat Systems: Volume 6. Systems Engineering and Platform Integration.* Monterey, CA: Naval Postgraduate School.

Hatzakis, Steven. 2019. “Best cTrader Brokers for 2019.” ForexBrokers.com. July 24, 2019. https://www.forexbrokers.com/guides/ctrader-review.

International Council on Systems Engineering (INCOSE). 2015. *Systems Engineering Handbook*, 4th ed. San Diego, CA: INCOSE.

Mann, Paul. 2019. *ISEA of the Future.* PowerPoint Presentation, Naval Surface Warfare Center Port Hueneme Division, Oct. 8, 2019.

Navy News Service. 2015. “U.S. Navy History and Week in Review.” November 20, 2015. https://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=7137.

Office of the Deputy Assistant Secretary of Defense for Systems Engineering. 2017. *Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs*. Washington, DC: Government Printing Office.

RAM Electronics. n.d. “Arduino Mega 2560.” Accessed November 8, 2019. https://ram-e-shop.com/.

Souvannason, Samuel. 2014. “Fleet Operations Center.” U.S. DEPT OF DEFENSE. December 14, 2017. https://www.defense.gov/observe/photo-gallery/igphoto/2002050290/.

Telkom Indonesia. n.d. “TELKOM 3S Profile.” Accessed November 8, 2019. http://www.satelittelkom3s.com/.

Turbosquid. n.d. “Destroyer UUS Zumwalt DDG-1000 with SH60 and MQ8B.” Accessed November 8, 2019. https://www.turbosquid.com/3d-models/3ds-max-uss-zumwalt-ddg-1000-destroyers/806941.

Wikimedia Commons. 2015. “US Navy 100721-N-0569K-007 Operations Specialist 3rd Class LaShawn E. Sloan monitors a radar system aboard USS Enterprise (CVN 65).” March 25, 2015. https://commons.wikimedia.org/wiki/File:US_Navy_100721-N-0569K-007_Operations_Specialist_3rd_Class_LaShawn_E._Sloan_monitors_a_radar_system_aboard_USS_Enterprise_(CVN_65).jpg.

Wikipedia. n.d. “Lockheed C-130 Hercules.” Accessed November 8, 2019. https://en.wikipedia.org/wiki/Lockheed_C-130_Hercules.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California